**From:** CIO-Sec-mailbox (MULTIUSER)
**Sent:** 07 August 2013 19:17
**To:** XXX XXXXXXXXXXXXX
**Subject:** Release-authorised: 20130807-FOI-XXXXXXXXXX-11-07-2013-152443-005-U

Ref No: 11-07-2013-152443-005

Dear XXXX XXXXXXXX,

Thank you for your letter of 11 July 2013 where you requested the following information:

> *"(1) As you will appreciate, this leaves the general public with the understanding that it is impossible to provide any computer records from MoD IT systems that were operating outside the UK in 2004, because the servers were cleansed of data. Can you clarify whether this is an accurate reflection of the policy of the Ministry of Defence as of 2004?*
>
> *(2) If so, can you clarify whether such a policy is still in force?*
>
> *(3) Please provide any documents which describe the policies and/or procedures in force in 2004 relating to the retention of information on the servers of Ministry of Defence IT systems that are returned to the UK.*
>
> *(4) Please provide any documents which describe the policies and/or procedures in force from 2005 – 2013 relating to the retention of information on the servers of Ministry of Defence IT systems that are returned to the UK.*
>
> *(5) If the above-referenced policies and/or procedures differ on the basis of which country the MoD has been operating in, please provide only the policies relevant to Iraq and Afghanistan."*

I am treating your correspondence as a request for information under the Freedom of Information (FOI) Act 2000. In accordance with section 1 of the FOI Act, I can confirm that the Ministry of Defence holds the requested information.

In response to your questions (1) and (2), your statement does not accurately reflect MOD policy in 2004. Material deemed worthy of preservation was printed off and incorporated into the (hardcopy) operational / corporate record, in accordance with Joint Service Publication 441: Defence Records Management Manual (JSP 441) and the Land Component Handbook. In addition, while some servers were cleansed of data and redeployed, an electronic archive capability had been put in place.

The policy continues to evolve as the type and amount of data changes over time. Records are now recovered from theatre at regular intervals, so that they can be retrieved to support appropriate activities.

Regarding your questions (3) and (4), in 2004, overarching MOD records management policy was promulgated in JSP 441 Version 2 dated March 2003. It was revised in 2007 and 2011. A copy of the 2003 (redacted) and 2007 revisions are attached to the covering email. The exemption at section 40(2) (Personal information) of the Act has been applied and the names of a number of junior officials have been redacted from the 2003 version of JSP 441 in line with the Department's policy on the protection of the identities of junior officials (i.e. those officials who carried a rank below that of Senior Civil Service or Military equivalent and are not sufficiently senior for their names to be a matter of public knowledge). Section 40 is an absolute exemption and does not require a public interest test to be conducted. The 2011 revision to JSP 441 is exempt from disclosure under Section 21 of the Act because it is already accessible to you by other means. It is already in the public domain, and can be accessed from the following hyperlink: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62750/jsp441_defence_records_mgt_policy_procedures_v4_2.pdf.

Further to JSP 441, each of the three Services which comprise the UK Armed Forces promulgates their own Operational Record Keeping policies. Operational records are high value records. They are a subset of all the information created on operations and are defined by the Single Service Operational Record Keeping policies. Operational records provide a body of information that can be used by the Single Service Historical Branches for historical operational analysis to support MOD decision making, they provide a basis for much of the record required to assist legal activity involving the Department and they are also the records of operations that MOD will transfer to The National Archives for permanent preservation.

Royal Navy operational records were still being stored in hard copy in 2004 following the guidance promulgated in the 1984 Queen's Regulations and Admiralty Instructions, paragraph 2909 (Reports of Proceedings). This paragraph is attached at Annex A. A new Operational Record Keeping policy for the Naval Service (Book of Reference (BRd) 9461) was first promulgated in November 2007. It was at that point that the Royal Navy moved to a system of Monthly Unit Records rather than the periodically written Reports of Proceedings which had existed prior to that date. The 2007 revision to BRd 9461, which has had section 40(2) of the Act already applied to it, is exempt from disclosure under Section 21 of the Act because it is already accessible to you by other means. It is already in the public domain, and can be accessed from the following hyperlink: http://www.bahamousainquiry.org/linkedfiles/baha_mousa/module_4/mod_4_witness_statem/exhibit_kedb/miv003727.pdf.

This document was further revised in 2011, and a redacted copy of this is attached. The exemption at section 40(2) of the Act has also been applied to the 2011 version of BRd 9461, and the names of a number of junior officials have been redacted.

The Queen's Regulations for the Army, paragraph 5.555 (Operational Records) requires the maintenance of an operational record whilst on active operations. This paragraph is attached at Annex B. In 2004, Army operational record keeping policy was promulgated in the Land Component Handbook, a copy of which you will find attached. A Headquarters Land Forces Mounting Order for Op Telic was published in May 2003 that also described the requirement to keep operational records. An extract from this Mounting Order can be found at Annex C. The Land Component Handbook was superseded by Land Forces Standing Order 1120: Operational Record Keeping (LFSO 1120) in 2005 and the 2009 revision is the latest version.

The exemption at section 40(2) (Personal information) of the Act has been applied and the names of a number of junior officials have been redacted from the 2005 and 2009 versions of LFSO 1120 in line with the Department's policy on the protection of the identities of junior officials. The 2009 revision to LFSO 1120 is exempt from disclosure under Section 21 of the Act because it is already accessible to you by other means. It is already in the public domain, and can be accessed from the following hyperlink:
http://www.bahamousainquiry.org/linkedfiles/baha_mousa/module_4/mod_4_witness_statem/exhibit_kedb/miv003708.pdf.

In 2004, the requirement to keep and maintain an RAF Operations Record Book was promulgated in paragraph 2137 of the Queen's Regulations for the Royal Air Force, an extract of which can be found in Annex D. The Air Publication 3040 (AP3040), which provides guidance on maintaining the RAF Operations Record Book, has not been amended since 2004 and therefore remains extant guidance for compiling RAF operational records. The RAF Operational Record Book is exempt from disclosure under Section 21 of the Act because it is already accessible to you by other means. It is already in the public domain, and can be accessed from the following hyperlink:
http://www.bahamousainquiry.org/linkedfiles/baha_mousa/module_4/mod_4_witness_statem/exhibit_kedb/miv003755.pdf.

In response to your question (5), I can confirm that the procedures did not and do not differ on the basis of in which country the MOD has been operating.

If you are not satisfied with this response or you wish to complain about any aspect of the handling of your request, then you should contact me in the first instance. If informal resolution is not possible and you are still dissatisfied then you may apply for an independent internal review by contacting the Deputy Chief Information Officer, 2nd Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail CIO-FOI-IR@mod.uk). Please note that any request for an internal review must be made within 40 working days of the date on which the attempt to reach informal resolution has come to an end.

If you remain dissatisfied following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not investigate your case until the MOD internal review process has been completed. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website, http://www.ico.gov.uk.

Yours sincerely,

***XXXXXXXXXXXXXXXXXXXXX***
***CIO-Sec Plans***

***☎Tel:      XXXXXXXXXXXXXXXXXXXXX***
***🖱Email:   CIO-SecPlans@mod.uk***
***✉Mail:    MB XXXXXXXXXX***

This Page Last Updated:
Tuesday, 11 March 2003 12:59

✉ Queries, Suggestions, etc.

# JSP 441
# Defence Records Management Manual

## CONTENTS

***See the new version of Chapter 6 containing updated policy on management of electronic records***

## Foreword by Head of DG Info-Records

Information is a valuable resource, one of the most valuable resources we possess. Without access to the right information it is impossible for us to do our jobs effectively.

In an organisation like MOD we are all constantly bombarded by information. Without effective records management we would quickly drown in this sea of information. It has never been more important to ensure that we identify the information which is valuable to us and store it in a way which allows us to retrieve it quickly when we need it. Equally, information which is less significant or ephemeral must be identified and disposed of when it is no longer needed.

No organisation can justify the expense of retaining information which has ceased to have value. In addition to the high storage cost, and the typical annual charge for office space in MOD HQ buildings is upwards of £500 per square metre, there is also the loss of efficiency as valuable information is lost from sight amongst the dross.

This manual sets out MOD records management policy. It identifies effective methods of storing Information in a coherent manner and of reviewing and disposing of information in an efficient and cost effective way. It also sets out our statutory obligations under the Public Records Acts of 1958 and 1967.

It is intended for all MOD staff, military and civilian. Where there are legitimate differences in procedure these are made clear but, in the main, the procedures are intended to apply to all so as to ensure a coherent and uniform standard throughout the Ministry.

Many of us are now routinely using IT networks such as CHOTS and increasingly we will wish to maintain records in electronic form. I would particularly draw your attention to Chapter 6 of the manual which sets out a framework for the maintenance of electronic records but stipulates that at present such records must be forwarded to DG Info-Records in hard-copy form. The Public Record Office is in the process of establishing arrangements for the permanent preservation of electronic records. When definitive guidance is available Chapter 6 will be amended to incorporate the criteria for the transfer of such records..

This manual provides clear and comprehensive guidance on records management and I commend it to you.

**Head of DG Info-Records**
**MOD Departmental Records Officer**

Home About This Manual Top of Page Index

Last updated: 11/03/03

**6749 hits since 5.3.02**

Queries, Suggestions, etc.

**JSP 441** **Defence Records Management Manual**

# ABOUT THIS MANUAL

This manual is intended as a reference source offering comprehensive guidance on the policy and procedure governing records management in MOD. Like all other government departments, MOD is bound by legislation governing the management of the records we create. This manual defines our legal obligations, explains how the task of managing the records we produce is co-ordinated, and identifies the role and responsibilities of branches.

- This manual defines the policy which applies throughout MOD, ie within MOD HQ and other civilian branches as well as Service formations and units and Defence Agencies. Where the regulations governing different parts of MOD vary this is made clear.

- The term 'branch" is used for convenience in this manual as a reference to each part of a Directorate or Service formation which maintains a discrete file list and which is responsible for the opening, closing and reviewing of files. Civilian ranks are also used for convenience and should be taken to equate to their Service equivalent where appropriate.

- This manual supersedes the elements of MOD Manual 2 "Getting it Done" which deal with records management policy, ie pages 12 to 15 of Section I and all of Section 7 "Records - Review and Disposal" (incorrectly identified as Section 6 on the Contents page). It also supersedes JSP 355. It should be read in conjunction with Volume 1 of JSP 440, the Defence Manual of Security.

Home JSP 441 Contents Chapter 1 Index

Last updated 11/03/02

**JSP 441** Defence Records Management Manual Chapter 1

This Page Last Updated: Wednesday, 05 March 2003 13:50

Queries, Suggestions, etc.

# Underpinning Legislation

## 1.1 Background

1.1.1 The public records of the United Kingdom date back to the 11th century and form a rich archive which is a part of our national heritage. The great wealth of documents and other records stored in the Public Record Office (PRO) have led to its recognition as one of the most significant archives in the world.

## 1.2 The Law

1.2.1 The law on public records is set out in the **Public Records Acts of 1958 and 1967**. Public records are defined in the Acts as "administrative and departmental records belonging to Her Majesty's Government, whether in the United Kingdom or elsewhere". These include electronic and paper records, photographic material, film, video, and samples and models which have been made for the purpose of conveying and recording information.

1.2.2 The Public Records Act of 1958 places a responsibility on all government departments to review the records which are generated within the department, to select those which are worthy of permanent preservation and transfer them to the Public Record Office, and to destroy all records which are not selected. The 1958 Act stipulated that all surviving public records should normally be released to the public 50 years after their creation; the Public Records Act 1967 reduced that period to 30 years.

1.2.3 There are exceptions to the 30 year release rule, usually on the grounds of an ongoing administrative requirement or continued sensitivity. However, all such exceptions need to be approved by the Lord Chancellor who is the Minister responsible for public records. It is also permissible for records to be held in places other than the PRO (known as "approved places of deposit") but, again, the Lord Chancellor's approval must be obtained.

1.2.4 The **Freedom of Information (FOI) Act 2000** will, for the first time, give a statutory right of access to information held by public authorities. The Act also requires information to be released proactively though a Publication Scheme. The FOI Act 2000 both provides a statutory general right of access to information and requires public authorities to publish information proactively through a Publication Scheme. TLB FOI Focal Points will constitute a centre of FOI expertise within the TLB area and form the core of a network for efficient pan-MOD handling of requests for information.

1.2.5 The FOI Act applies to all parts of MOD including the armed forces, agencies and trading funds, whether they are located in the UK or overseas.  Only the special forces and any units actively providing assistance to GCHQ are outside its scope.

1.2.6 The Act introduces a general right of access to information held by public authorities and also creates an obligation for those authorities to release information proactively by adopting and maintaining a Publication Scheme. Implementation will be in two main phases. In phase one, different types of public authority will gradually be required to establish their Publication Schemes: government department Schemes must be in place by the end of November 2002.  In the second phase, the right of access to information on request will become effective.  All public authorities will have to honour this right from January 2005.

1.2.7 The MOD policy lead on issues relating to openness, including implementation of the FOI Act rests within DG Info with AD InfoExp-Access. For more information about FOI see Annex A and visit the DG Info Access MODWeb site.

1.2.8 The **Data Protection Act 1998** (DPA) is the result of a European Directive on Data Protection, which requires Member States to "protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data". All Service and civilian members of staff are bound by its provisions, which confer certain rights and responsibilities. The Act applies to all parts of the UK.

1.2.9 The DPA is about access by individuals to personal data held on them by any organisation whereas the FOI Act relates to the disclosure of information held by public authorities. Responsibility for ensuring the implementation of the DPA throughout MOD lies with the Director Claims and Legal (Finance and Secretariat). For more information about the implications of the DPA visit the CL(F&S) MODWeb site.

## 1.3 The Responsibility for Public Records Within MOD

1.3.1 Under the terms of the 1958 Act each government department is required to appoint a Departmental Records Officer who is responsible for ensuring that the records generated within their department are properly reviewed and that the appropriate records are selected for permanent preservation and transferred to the PRO. Head of DG Info-Records is the MOD Departmental Records Officer and is also the Chief Registrar.

1.3.2 The Departmental Records Officer is responsible for ensuring the cost effective organisation and control of MOD records throughout their life.

## 1.4 What Are Public Records?

1.4.1 It is important to understand that all documents generated by government departments are public records covered by the terms of the Public Records Acts, This does not mean that all documents will be worthy of permanent preservation. There would be no logic in simply keeping everything. The task of each department is to select those documents which merit capture as records and to safeguard them accordingly. Subsequently decisions must be made about the length of time for which records should be retained to meet administrative needs - this must take into account such issues as legal or contractual requirements.

1.4.2 Once the administrative need to retain a record has ceased a decision needs to be made as to whether the records have historical value and merit permanent preservation in compliance with the Public Records Act. For MOD this task is undertaken by DG Info-Records, taking into account the recommendation made by the originating business unit..

1.4.3 The following definitions are helpful:

**Documents** are defined as any tangible information received or produced by the department.

**Records** are those documents that support some official activity or decision and need to be preserved for future reference.

***But remember - legally, any document produced by or held by MOD is a public record***.

## 1.5 The Importance of Records to MOD

1.5.1 The MOD and the Armed Services are large and complex organisations. Their decisions and actions affect many people, potentially over long periods. The various Business Units of MOD have an obvious need to record their decisions and actions for their own and wider MOD use. These decisions and actions are however increasingly open to legal, Parliamentary, media and personal challenge, often many years after the event. Business Units, whether it be the originator of the action or a successor branch, need to know what happened and why it is important. Selection of records for medium and long term preservation for administrative use needs care, foresight and experience; the judgements made at this stage must also be tempered with the need for the permanent preservation of some records, as mentioned above, for the national record in the PRO. If Business Units are in doubt over which of their existing records need to be kept for medium and long term use, advice and help should be sought from DG Info-Analysis/Records and also from the

1.5.2 Service Historical Branches, who have wide experience of the use of records by MOD Ministers, Business Units, the Services and also of the interests of historians, the media and the public in these records subsequent to their opening after 30 years. If in doubt, err on the side of caution and forward the material to DG Info-Records with a recommendation that it be considered for permanent preservation.

Home Back to Contents Top of Page Annex 1a Index

Last updated 05/03/03

PUBLIC RECORD OFFICE

The Public Record Office (PRO) has custody of the archival heritage of the British state. Its holdings consist of the legal, administrative and departmental records of England and Wales, and the United Kingdom Government. The earliest public record is Doomsday Book (1086) and they extend to the present day. They form one of the most complete and extensive archives in the world. The records currently occupy over 160 kilometres of shelving, to which, on average, between one and a half and two kilometres of fresh transfers are added each year. All these records provide information that is an element of good governance. They assure the accountability of government over time. They provide a sound basis for historical and genealogical research. They can be used as legal evidence and they extend knowledge of past actions and decisions to inform future decision-making. In carrying out its duties, the PRO serves the needs of present and future generations. As the national archive for England, Wales and the United Kingdom, the Public Record Office (PRO) acts in large part as the nation’s memory.

The PRO became an Executive Agency on 1 April 1992. It operates as a separate government department under the Lord Chancellor, who appoints the Keeper of Public Records. The PRO’s statutory aims are defined by the Public Records Acts 1958 and 1967.

The function of the PRO is to discharge the duties laid on the Keeper of Public Records by the Public Records Acts, in the most economical, efficient and effective manner. The ‘public records’ are records of government departments, courts, tribunals and certain other public bodies defined in the Public Records Act 1958 (as amended). They comprise not only written records but records conveying information by any means, including maps, seals, photographs, moving images, sound recordings and electronic records.

Back to DG Info-Records    Home    Back to DG Info-Records DRO    Public Records Acts

Last updated 11/03/02

This Page Last Updated:
Friday, 11 October 2002 12:24

Queries, Suggestions, etc.

| JSP 441 | Defence Records Management Manual Chapter 1 Annex A |
|---|---|

# Freedom of Information Act 2000

**Note: Lead responsibility for MoD FOI policy rests with DG Info-Access**

The Freedom of Information Act (FOI) 2000 will, for the first time, give a statutory right of access to information. This will entitle any person to be told upon written request whether MOD holds particular information, and, assuming that we do, to have that information communicated to them within twenty working days. The Act also requires all public authorities to maintain a Publication Scheme, and to release information proactively in accordance with its terms.

The Act must be fully implemented by the fifth anniversary of its Royal Assent (on 30 November 2000). The Lord Chancellor announced on 13 November 2001, however, that it was the Government's intention to implement the Act fully by January 2005. On this date, all public authorities must comply with the general right of access to information. The requirement for Publication Schemes will be implemented on a gradual basis, commencing in November 2002.

All parts of MOD, including the Armed Forces, the MDP, agencies, trading funds and NDPBs, will be subject to the provisions in the FOI Act. It will also be possible for some contractors engaged by MOD to brought within its terms. Only the Special Forces and any units that are actively providing assistance to GCHQ are outside the scope of the Act.

**How does the Lord Chancellor's implementation plan relate to MOD?**

Under the timetable announced by the Lord Chancellor, MOD is required:

- By November 2002 - to have in place a Publication Scheme relating to MOD as a government department and to NDPB's subject to the Code of Practice on Access to Government Information.

- By June 2003 - to have in place a Publication Scheme relating to the Armed Forces and MDP.

- By February 2004 - to have in place a Publication Scheme relating to the NDPB's not subject to the Code of Practice on Access to Government Information.

- By June 2004 – to have in place a Publication Scheme relating to any contractors brought under the Act by an Order from the Lord Chancellor.

- By January 2005 - to comply with the provisions relating to the general right of access to information.

Within MOD, the intention is to prepare a Publication Scheme for November 2002 that includes the entire department, including the Armed Forces and MDP, within its scope.

**The Proactive Element: Publication Schemes**

The requirement to maintain a Publication Scheme is unique to the UK's FOI legislation. The objective is to encourage the proactive and continuous disclosure of information on topics of public interest. In practice, "publication" means making information reasonably accessible, and in most cases this is likely to be achieved by placing the information on an Internet site.

The Act says that public authorities must specify Classes of Information they intend to publish, say how this information will be made available and whether it will be available free or on payment. The Publication Scheme can be seen as a catalogue of the information MOD makes available. In practice, the intention is to provide a direct link from the Publication Scheme to any information that is published on the Internet.

A pilot of the Publication Scheme is available on the MOD Internet site. Although the details will be different in the full Publication Scheme, it is envisaged that the structure will be largely the same.

Once the Publication Scheme has been approved by the Information Commissioner, there will be a statutory obligation to publish information in accordance with the Classes of Information MOD has specified. The Information Commissioner has interpreted this to mean that any information that falls within the scope of a Class of Information must be published.

**The Reactive Element: The General Right of Access to Information**

Under the Code of Practice on Access to Government Information there is already a requirement to answer any request for information in accordance with prescribed rules, and to refuse information only if one of the specified exemptions applies. FOI gives this right to information a statutory basis, however, and creates a more exacting enforcement regime.

Under the terms of the Act, any request for information that is received in permanent form (a letter, e-mail, fax etc) must be answered in accordance with the FOI disciplines. Requests can be made from anywhere in the world and will have to be handled in accordance with the Act regardless of which MOD unit receives the request. A letter sent to a military unit in Germany, the Falkland Islands or Cyprus will therefore have exactly the same status as one received in a Minister's office in London.

The Act requires that applicants give their name and address and describe the information wanted. They must then be notified whether MOD holds the information they have requested, and, if so, the information must be communicated to them. Depending on any preference expressed by the applicant, and whether it is "reasonably practicable" to comply, disclosure could take the form of a copy of the information in permanent form; a synopsis of the relevant documents; or an opportunity to inspect a record containing the information. A substantive response must be provided within twenty working days of MOD receiving the request.

There is also a duty under the Act to provide advice and assistance to applicants. It will not be acceptable to ask why the request has been made, but if it is not clear what information will best meet the request, the options must be discussed with the applicant.

**Does this mean everything must be released?**

No. The Act recognises that some information needs to be held back for reasons such as national security, defence, international relations, and the formulation of government policy. However, it does not provide a solid screen behind which we can shield information in these categories. A total of 23 categories of exemption are identified in the Act, but only a handful of these give an absolute right to withhold information.

The absolute exemptions that are likely to be most relevant to MOD are: information supplied by, or relating to, security bodies named in the Act; information that it would be an actionable breach of confidence to disclose; information that is personal data and therefore subject to the Data Protection Act 1998; and information that is already accessible to the public by other means (e.g. in the Publication Scheme).

The exemptions that are not absolute require information to be assessed for release with reference to the "public interest". This includes information relating to: national security, defence, international relations (including information supplied in confidence by a State or international organisation), the formulation of government policy, and commercial interests. In these cases, even if the information does fall within the scope of the exemption, it must be provided to the applicant unless it is judged that the public interest in withholding the information outweighs the public interest in disclosure.

It should be noted that it will not be possible to withhold information simply because it has a security classification. FOI is classification blind, and it will be necessary to consider even Top Secret information on a case-by-case basis, should it be within the scope of a request. The only legitimate basis for withholding information will be if this has been properly considered and justified in the context of an FOI exemption.

In cases where the applicability of an exemption is being assessed in the light of the public interest, it will be permissible to provide an interim response within the twenty working days. This reply will have to quote the exemption that the information falls under, and notify the applicant of the date by which they can expect to receive a substantive answer.

**The Enforcement Regime**

The Freedom of Information Act creates the position of Information Commissioner (IC). This subsumes the role of the Data Protection Commissioner, and creates one post that will have responsibility for oversight of both the Data Protection Act and the FOI Act. The Information Commissioner is an independent official who reports directly to Parliament. The current Information Commissioner is Elizabeth France.

The IC has a number of roles. She will approve Publication Schemes and promote good practice in accordance with the Lord Chancellor's Codes of Practice (relating to records management and the discharge of functions by public authorities). In addition to this, she will be able to issue information, decision and enforcement notices to enforce compliance with the general right of access.

In practical terms, if a request for information is refused, it will be necessary to inform the applicant not only which exemption the information is being withheld under, but also of the appeals process. The first step of this process will be an internal review, but if the applicant remains unhappy following this they will be able to appeal to the Information Commissioner. After investigation, She will then have the power to order disclosure of information that she feels has been incorrectly withheld.

**So what is new?**

The main differences between the FOI Act and the Code of Practice on Access to Government Information are:

- The FOI Act is part of the law of England, Wales and Northern Ireland; the Code is non-statutory.
- Under FOI the applicant may request information in the form of a copy of the documents, a synopsis of the relevant

information or the opportunity to inspect a record containing the information.

· Under FOI there is a statutory requirement to respond to requests for information within working days.

· The Act imposes a duty on public authorities to assist people to identify the information they are seeking, and there is no entitlement to ask why the information is wanted.

· The Information Commissioner, a new post established by the Act, will have power to order disclosure of information.

- The requirement for public authorities to proactively publish information through a publication scheme. These schemes will have to be approved by the Information Commissioner.

**What about Data Protection?**

The Data Protection Act 1998 (DPA '98) deals with access by individuals to personal data held on them by any organisation. The Freedom of Information (FOI) Act 2000 relates to information which is not personal to the applicant held by any public authority. Responsibility for ensuring the implementation of Data Protection Act 1998 (DPA 98) throughout MOD lies with the Director Claims and Legal (Finance and Secretariat). For more information about the implications of the DPA is at http://www.chots.mod.uk/policy/DPO/default.htm

**Further Information and Lead Responsibility**

Lead responsibility for MOD FOI policy rests with DG Info Access. A great deal of information, including the answers to some Frequently Asked Questions, is available on the DG Info MODWEB site at http://centre.defence.mod.uk/dgi/FOI/Access.htm . Further guidance will be issued in due course, not only by MOD, but also by the Information Commissioner and the Lord Chancellor’s Department, which has the pan-Government lead on FOI. It is important to remember, however, that the provisions relating to the general right of access will not take effect until January 2005. Further guidance on how to handle requests for information will be issued before then.

In addition to this, there are FOI Focal Points in each TLB (for Centre TLB the Focal Points are at HLB level). One of their responsibilities is to spread awareness of FOI through the management areas they represent, and they will be able to provide further information and explanation about preparations for FOI in your area.

**Final thoughts for now . . .**

The Freedom of Information Act will clearly impact on the way that MOD answers requests for information. In order for the Act to be successfully implemented there will need to be both a cultural shift and improved working practices.

Under FOI, it will be necessary to have a ‘need to share’ rather than a ‘need to know’ culture. The more information that is made proactively available, the fewer the number of requests that we are likely to receive.

The ability to answer requests for information within twenty working days will be dependent upon effective and efficient record management. We will not be able to provide information to the public if we can not locate it ourselves. Such a scenario will not be viewed sympathetically by the Information Commissioner.

There is a great deal of work to be done before the Act comes into force to ensure that we can comply with the new law. It is important to remember, however, that the provisions relating to the general right of access will not come into effect until January 2005. We can also take comfort from the fact that other countries that have implemented FOI legislation - for example, Canada, New Zealand, Australia, Ireland and of course, the USA - have not come to a grinding halt by opening up their information holdings!

Text last updated : 13 September 2002

Home Back to Contents Top of Page Chapter 2 Index

Last updated 11/10/02

**JSP 441** **Defence Records Management Manual Chapter 2**

This Page Last Updated:
Friday, 24 January 2003 12:20

Queries, Suggestions, etc.

# Role and Responsibilities of DG Info-Records

## 2.1 Responsibility for Records Management Within MOD

2.1.1 As Departmental Records Officer (DRO) Head of Info-Records is responsible for ensuring that the department's records are managed effectively and that the appropriate records are identified and passed to the Public Record Office.

2.1.2 As Chief Registrar, the DRO is responsible for the establishment of procedures governing registry practice. These procedures are designed to achieve the cost-effective organisation and control of records from the time of their creation, through their use and storage, to their destruction or preservation by the PRO. In establishing these rules the DRO consults with other branches such as the security branches, where appropriate.

2.1.3 The DRO is responsible for MOD's records storage facilities at Hayes and Central London, for the central review and assessment of records to determine whether they merit permanent preservation, for the registry advisory service and for the conduct of records management audits. Overall the DRO is supported by around 130 staff.

2.1.4 The DRO is also responsible for the production of this Records Management Manual which details the minimum standards to be adhered to by all MOD business units and also identifies good records management practice.

2.1.5 Info-Records is also responsible for the approval of the Main Headings and numbers for all MOD HQ (and other civilian business unit) file lists, including changes and amendments to established lists.

## 2.2 Organisation of Info-Records

2.2.1 The following diagram indicates the structure of Info-Records and identifies the key responsibilities of each part of the business unit.

| | **Head of Info-Records (B2)**<br>DRO and Chief Registrar | | |
|---|---|---|---|
| **Info-Records1 (C2)** | **Info-Records2 (C1)** | **Info-Records3 (C2)** | **Info-BCTEDRM1 (C1)** |
| Review, listing and transfer of records to the PRO. Access and release questions. Management of Sensitive Archive at Old War office. | Storage of MOD records at Hayes. Provision of retrieval service for MOD and Service business units / units. Release of records and information. | Records management advisory service. Records management audits. Approval of business unit file lists. Sponsor of JSP 441. | Formulation of MOD strategy and policy governing management of electronic records. |

## 2.3 Role of Info-Records1

2.3.1 Info-Records1 is responsible for the review of records which are forwarded from business units. Records are normally reviewed twice, once around 5 years after they are closed (if they have been forwarded by the originating business unit by that time) and again 25 years after their closure. It is through this process of review, incorporating the recommendation made by the originating business unit, that those records worthy of permanent preservation by the Public Record Office (PRO) are selected. Info-Records1 is also responsible for the approval of business unit Disposal Schedules.

2.3.2 Once records have been selected for the PRO, they have to be prepared for dispatch. This involves preparing a detailed inventory of the material, placing it in the appropriate boxes for storage at the PRO, and indexing it (where applicable). This is referred to as the "listing" process.

2.3.3 Info-Records1 is also responsible for the archive in central London which houses TOP SECRET and other sensitive material.

2.3.4 In addition, Info-Records1 responds to questions about the status of MOD records from other government departments, overseas governments and members of the public.

2.3.5 Info-Records1 is based at Great Scotland Yard and can be contacted on 70254 MB. Contact points for the archives administered by Info-Records1 are at Chapter 8, para 8.4.

## 2.4 Role of Info-Records2

2.4.1 Info-Records2 is responsible for the management of the MOD archives at Hayes in Middlesex. The archives house most of the records in registered files along with unregistered records and a large quantity of Service personnel records and scientific and technical material. Personnel records are kept for an extended period, with the Lord Chancellor's authority, as reference may need to be made to them for many years after discharge, for instance, for pension purposes. Additionally, Info-Records2 deals with many enquiries from non-MOD sources, including ex-service personnel and their relatives.

2.4.2 Civilian personnel records which, like Service records, are retained for an extended period, are housed in Llangennech, Dyfed, and are managed by DSDC(L) on behalf of the Head of Info-Records.

2.4.3 Contact points for Info-Records2 are at Chapter 8, para 8.7.1.

## 2.5 Role of Info-Records3

2.5.1 Info-Records3 is responsible for provision of advice and guidance to business units on MOD records management policy through the provision of a **Records Management Advisory Service**. Info-Records3 is also responsible for the production of this Manual.

2.5.2 Info-Records3 is also responsible for the approval of the main headings and numbers used by all MOD HQ (and other non-Service) business units including any subsequent amendment. Additionally, the structure of the file list must also be approved (see Chapter 4, para 4.4.1).

2.5.3 Info-Records3 also carries out **Records Management Audits**, designed to ensure that business units are adhering to the regulations contained in this manual. After each inspection a report is forwarded to the Business Unit Head identifying any areas which require attention and any other remedial action necessary.

2.5.4 Info-Records3 is based at St Giles Court and can be contacted on 70250 MB, 70251 MB and 70252MB.

## 2.6 Role of Info-BCTEDRM1

2.6.1 Info-BCTEDRM1 [formerly Info-Records4] is responsible for provision of advice and guidance to business units on MOD strategy and procedures governing the management of electronic records. (see Chapter 6 )

2.6.2 Info-BCTEDRM1 is based at St Giles Court and can be contacted on 84405MB and 85669MB.

Home Back to Contents Top of Page Chapter 3 Index

Last updated 24/01/03

**JSP 441** **Defence Records Management Manual Chapter 3**

**This Page Last Updated:**
**Monday, 27 January 2003 12:21**

Queries, Suggestions, etc.

# Responsibilities of MOD Headquarters Business Units, Other Civilian Establishments, Service Commands and Units

***Note that the term "branch" is used generically in this chapter to mean business unit, Service unit, or any other organisation maintaining a discrete file list.***

## 3.1 The Role of the Directorate / Agency Records Officer

3.1.1 Each Directorate or Agency is responsible for the maintenance of the records it generates or receives. It is imperative that these records are managed efficiently and maintained in a way which allows ready access to those which are needed, while those records which are no longer of value are dispensed with (e.g. forwarded to DG Info-Records or destroyed).

3.1.2 The retention of records which are unlikely to have any further administrative value and have no historical value leads to unnecessary storage costs and wasted effort in further review.

3.1.3 The maintenance of an effective system of record keeping requires a systematic approach to the management of the task. Registry staff and desk officers all have a part to play but it is important that the task is co-ordinated at management level.

3.1.4 Each Directorate / Agency should appoint a **Directorate Records Officer** [**DIRO**] / **Agency Records Officer** [**ARO**] to ensure that effective records management procedures are put in place and maintained. The **DIRO** / **ARO** will also be responsible for co-ordinating the activities of subordinate Branch Records Officers (see para 3.2 below) and will be the prime point of contact with DG

Info-Records. Appointees should normally be at C1 (or Service equivalent) level. Directors / Chief Executive's should ensure that full contact details for the **DIRO** / **ARO** are forwarded to DG Info-Records 3 and that these are updated to reflect any subsequent change .

3.1.5 The **DIRO** / **ARO** must ensure that:

- **Branch Records Officers** [**BRO**] of the appropriate grade (normally Band C2 / Service equivalent) have been appointed in subordinate branches and that they are familiar with their role and responsibilities (see Note 1 below)
- all Branch File lists have been approved by DG Info-Records3 and copies have subsequently been submitted to DG Info-Records3 for retention (see chapter 4, para 4.4) [Note that this is not required within Service formations.]
- all **BROs** have produced a Branch Disposal Schedule and forwarded a copy to DG Info-Records3 (see chapter 5, para 5.4)
- **BROs** have suitable procedures in place to ensure that all new staff have received any required records management training
- efficient and timely review of registered files (and material held other than on such files) is being undertaken ( see chapter 5, para 5.5)
- an up to date list of all **BROs** in their area is maintained and full contact details have been forwarded to DG Info-Records3
- newly appointed **BROs** are briefed on their role and responsibilities
- they act for the Director/Chief Executive in matters related to Records Management Audits conducted by DG Info-Records3, e.g.:
  - responding to the initial audit request letter and agreeing a suitable audit programme;
  - following receipt of the audit report, take prime responsibility for ensuring that the relevant recommendations are incorporated into an action plan indicating appropriate timescales for completion of the required actions;
  - when the audit has taken the form of a sampling exercise, which will typically be the case within larger Directorates and Agencies, ensuring that all **BROs** are apprised of the required remedial actions and are tasked with assessing compliance within their areas.
- the need for local records management instructions to augment those contained in JSP 441 has been assessed and that any such instructions are consistent with JSP 441 and are issued throughout the organisation
- suitable monitoring arrangements are put in place to ensure that effective records management procedures are embedded and maintained.

[Note 1: In this context the term "branch" should be taken to refer to each part of a Directorate or Service formation which maintains a discrete file list and is responsible for the opening, closing and reviewing of files.]

3.1.4 If the **DIRO** /**ARO** determines that there is major weakness in the existing records management procedures within the branch it may be appropriate to recommend that a suitable change objective be incorporated into the Management Plan.

## 3.2 The Role of the Branch Records Officer

3.2.1 The **Branch Records Officer** [**BRO**] is responsible to the **DIRO** /**ARO** for the following functions:

- the creation and maintenance of the branch File List (see Chapter 4, para 4.5);
- the maintenance of a definitive record of material held by the branch which is not located on registered files (see Chapter 4, para 4.21);
- the co-ordination and maintenance of a Disposal Schedule identifying, where possible, the appropriate retention period and method of disposal of branch records - e.g. either destruction or archiving (see Chapter 5, paras 5.3 and 5.4). The Branch Records Officer may be given responsibility for the completion of all Registered File Disposal Forms (MOD Form 262F), consulting the relevant desk officer as necessary. Alternatively, this task may be carried out by desk officers;
- forwarding a copy of the branch Disposal Schedule to DG Info-Records3 where it will be retained for future reference (see Chapter 5, para 5.4.6);
- ensuring that comprehensive local instructions exist covering the working practices in the registry and that new members of staff receive suitable training upon arrival;
- line management of registry staff

3.2.2 It is important to ensure that the **BRO** has sufficient authority within the organisation to discharge their responsibilities, including the signing off of MOD Form 262Fs. For that reason appointees should be at Band C2 (or Service equivalent) level and will usually have line responsibility for the Registry supervisor and staff. Depending on the size of the branch the registry may be supervised on a day-to-day basis by a Band D or a Band E1. That person will deal with much of the routine work of the section. However, the **BRO** retains responsibility for ensuring that the procedures outlined in this manual are adhered to. The **BRO** will also be the focal point for liaison with DG Info-Records.

## 3.3 The Role of the Registry Supervisor

3.3.1 The registry supervisor has day-to-day responsibility for the following:

- ongoing maintenance of the branch File List including the allocation of new file titles and numbers as required (see Chapter 4, para 4.2);
- maintenance of the registered files and other records held within the registry in accordance with the instructions in this manual and in JSP 440;
- the closure of registered files in line with the instructions at Chapter 4, paras 4.17 and 4.18;
- preparation of branch records for disposal in line with the branch Disposal Schedule (see Chapter 5, paras 5.3 and 5.4);
- maintenance of a system to record the whereabouts of registered files which have been removed temporarily from the registry (see Chapter 4, para 4.7);
- supervision of registry staff

## 3.4 The Role of Desk Officers and Other Business Unit Staff

3.4.1 Desk officers and other business unit staff raising or receiving official correspondence have a responsibility to ensure that anything which is not ephemeral is placed in the appropriate registered file. If the nature of the material makes it impossible to place in a registered file (for example, bulky material) then the nature and whereabouts of the material should be recorded.

3.4.2 Desk officers also have a responsibility to liase with the records officer when they request the creation of a new registered file (or any other type of record) to ensure that a suitable entry is made in the business unit Disposal Schedule (wherever possible). Subsequently, desk officers are likely to be involved in the completion of the Registered File Disposal Form (**MOD Form 262F**) which will ultimately confirm or amend the recommendation made in the business unit Disposal Schedule (see Chapter 5, para 5.3).

**Home** **Back to Contents** **Top of Page** **Chapter 4** **Index**

Last updated 27/01/03

This Page Last Updated:
Thursday, 03 April 2003 10:32

Queries, Suggestions, etc.

# JSP 441 Defence Records Management Manual Chapter 4

# The MOD Filing System

## 4.1 Registered Files

4.1.1 MOD, in common with other government departments, operates a filing system which makes extensive use of registered files. Each file relates to a particular subject, or aspect of a subject, and has a unique identifying reference (normally an alpha/numeric combination). Purpose-designed file covers are used.

4.1.2 All papers of substance should be placed on a registered file. Ephemeral papers, rough drafts, spare copies etc need not be placed on registered files if they are likely to be needed only temporarily and are not of any lasting significance. Such papers should be destroyed when no longer needed. If it transpires that such a paper is needed for an extended period, or has taken on a greater significance, it should be transferred to the appropriate registered file.

## 4.2 Preparation of a File List

*[Note: Paragraphs 4.2 to 4.4 outline the requirements within MOD HQ and other non-Service areas. Service formations and units may, at their discretion, maintain a file list based on historical precedent though they may choose to adopt the one outlined here.]*

4.2.1 The key to establishing an effective business unit file list is to approach the task logically and consistently. The guidance which follows relates to the creation of a new file list. While most business units will not need to create an entirely new file list very often business units involved in reorganisations or mergers may need to do so. For others, the underlying principles should still be applied when file lists are being amended or updated.

4.2.2 There are a number of ways in which a file list might be constructed. Within MOD HQ and other civilian business units the hierarchical structure is used. Such a system incorporates the use of "Main Headings" to identify the key activities of each business unit, with the use of subsidiary "Secondary Headings" and "Tertiary Headings" to identify more specific, subordinate, subjects.

4.2.3 In creating a hierarchical file list, the first task is to identify the Main Headings which will be required. It is impossible to be prescriptive about the main headings to be used, as they will be determined by the purpose and activity of each business unit. However, by convention, the first main heading on most file lists is "Administration" under which secondary headings might reflect such subjects as Staff, Security, Organisation and Training.

4.2.4 The remainder of the main headings, as dictated by the activity of the business unit, should be listed in order of significance.

4.2.5 The key to establishing an effective hierarchical file list is consistency. Having identified the main headings and listed them in order of importance, apply the same approach to the creation of subsidiary headings beneath each main heading. Ensure that activities which are linked appear together. An example is at Figure 4.1 below where three files are to be created, each dealing with a different aspect of business unit security.

4.2.6 The main heading is Administration, the secondary heading is "Security" and there are three tertiary headings, each dealing with a different aspect of security. Note that each element of the file title is separated by a dash (**-**). It is important to represent file titles in this way in the file list, on the file cover, and elsewhere. If this is not done there is a risk that the correct title will become lost over a period of time. This can lead to confusion and errors such as misfiling of documents.

**Figure 4.1**

| File Reference Number | Main Heading | Secondary Heading | Tertiary Heading |
|---|---|---|---|
| *** / * / *** | Administration - | Security - | Inspections |
| *** / * / *** | Administration - | Security - | Breaches |
| *** / * / *** | Administration - | Security - | Spot Checks |

4.2.7 In the example at Figure 4.1 the hierarchical structure has been reflected in the identification of business unit "**Security**" as an element of business unit **Administration**. In turn, three facets of business unit security have been identified, "**Inspections**", "**Breaches**", and "**Spot Checks**". To maintain the integrity of the file list, and to apply a logical approach, these three related subjects have been placed next to each other. By applying the same principle throughout the file list, a logical and straightforward file index will be created which is consistent and easy to follow.

4.2.8 To avoid file titles becoming cumbersome the title allocated to each file should not normally exceed three elements e.g. main heading, secondary heading, and tertiary heading. Where absolutely necessary the use of additional sub-headings is permissible.

4.2.9 Terms such as "**General**", "**Miscellaneous**" and "**Policy**" are too vague to be appropriate for use as main headings and should be avoided for use as secondary or tertiary headings wherever possible. All headings should be specific and should clearly identify the nature of the material to be contained within the file.

4.2.10 Use of abbreviations and acronyms should be avoided where possible. Where they are used the words represented must be included in full in the file title and the abbreviation / acronym inserted in brackets thereafter.

## 4.3 Allocation of a File Reference

4.3.1 Each file must be allocated a unique file reference. This will be an alpha/numeric combination which serves to ensure that the file which has been created is not confused with any other file. Each element of the reference should be separated by an oblique stroke (/) to distinguish each individual component.

4.3.2 The first element of the alpha/numeric file reference will be the business unit short title. Alternatively a directorate title might be used, or both might be used. If the business unit short title ends with a number, the number must be bracketed to avoid confusion with the file number.

4.3.3 The business unit title should be followed by the file reference number. The number of elements contained in the file title will dictate the number of elements in the numerical element of the file title. Thus a file entitled "**Administration-Security**" will have **two** numerical elements, while a file entitled "**Administration-Security-Inspections**" will have **three**. Note that all file titles should have at least two elements. Thus there will be no file entitled Administration" which is the main heading under which appropriate files will be opened.

4.3.4 All file titles should have at least two elements. Thus there will be no file entitled "Administration", which serves as the main heading under which appropriate files will be opened.

4.3.5 A full file reference for a file held by DG Info-Records might be:

- **DG INFO/1/2/3 Administration-Security-Inspections**

Note that the file number has three elements, corresponding to the number of elements in the file title. Though in this example each element of the file number is a single numeral, in practice each element may be a double or even triple number, as dictated by the overall number of files which have been created. The business unit file list should take the above form, listing first the file reference and then the full file title.

4.3.6 A common error when drafting a new file list is to leave unexplained gaps between file numbers, e.g. the main heading "Finance" is allocated the number "**3**" but the next main heading "Equipment" is allocated the number "**5**", the number "**4**" remaining unallocated. This is bad practice and, ordinarily, no gaps should be left when allocating numbers to main headings (or subsidiary headings). If a gap is unavoidable, the unused number should appear on the file list and should be annotated with the word "**RESERVED**".

## 4.4 Approval of Main Headings and Numbers and File Structure

4.4.1 **The main headings and numbers of all MOD HQ and other civilian business unit file lists must be approved by DG Info-Records3 before use, as must the structure of the file list**. Once approval has been granted the new file list should be constructed, e.g.. secondary and tertiary headings and full reference numbers should be allocated. **A copy of the full file list, incorporating a Disposal Schedule, is to be forwarded to DG Info-Records3 within 3 months of its introduction**. Subsequently any proposed changes to main headings or numbers must also be approved and an up to date copy of the file list is to be forwarded annually.

4.4.2 If the business unit short title to be used is unchanged from that used in the previous file system then the main heading numbers previously used cannot be used again. This is to avoid confusion resulting from the existence of files bearing the same file reference but different titles. In these circumstances the new main headings must be allocated numbers which do not clash with the previous system. For further advice on this topic contact DG Info-Records3.

4.4.3 Service formations and units have, historically, used different methods of referencing registered files and are not required to obtain approval from DG Info-Records3 before creating or amending file lists. However, they can be consulted for advice on all aspects of records management practice, including the adoption of the MOD HQ filing system.

## 4.5 Maintenance of an Approved File List

4.5.1 The **Business Unit Records Officer** (BRO) (see Chapter 3, para 3.2) should maintain a definitive copy of the file list which should be amended when new files are created. The BRO has ultimate responsibility for the maintenance of the list though day-to-day responsibility may be delegated to the registry supervisor.

4.5.2 The completed file list must incorporate a **disposal schedule recommendation** for all files. More information on creating and maintaining a **Disposal Schedule** is contained in Chapter 5, para 5.3.

4.5.3 The file list must also identify the "owner " of each file i.e. the desk officer responsible for the file and ultimately responsible for completion of MOD Form 262F - Registered File Disposal Form (see Chapter 5, para 5.5)

## 4.6 Maintenance of a Registered File

4.6.1 The full file title, as it appears in the file list, should be entered on the front cover of the file, along with the designated file reference. The opening date of the file is also to be recorded. Note that no file should be opened until there is an enclosure to be placed in it therefore the opening date will be the date of origin of the first enclosure.

4.6.2 If the file is a new part of an existing file which has been closed it should be allocated a part reference. The first part of any file will be Part A, though this letter should not be added to a file cover until a subsequent part is opened. The subsequent file will then be "Part B" and so on. If Part Z has been reached and there is a need to open a further part it should be opened as "Part AA" followed by "Part AB" and so on. The part number should not be included when recording the file reference on correspondence etc.

4.6.3 An example of a completed Registered File cover is at Annex A.

## 4.7 The Registered File Record Sheet (MOD Form 262A)

4.7.1 When a new registered file is opened its existence must be recorded on a "Registered File Record Sheet" (**MOD Form 262A**). An example of a **MOD Form 262A** is at Annex B. When a registered file is closed the date of closure is to be recorded on the MOD Form 262A along with the date of the last enclosure on the file (boxes are provided on the form for both dates).

4.7.2 The Registered File Record Sheet is the definitive record of a file's existence. If subsequent parts to the file are opened then a new 262A is to be raised for each part. They are to be placed in binders (**MOD Form 262**) and maintained until replaced by **MOD Form 262F**, "Registered File Disposal Form". (Guidance on completion of the Registered File Disposal Form is at Chapter 5, para 5.9).

4.7.3 If a registered file is sent temporarily to another business unit the Registered File Record Sheet must be used to identify to which business unit it was sent, on what date it was sent and the date on which it was returned.

4.7.4 The Registered File Record Sheet may also be used to record that a file has been issued to a member of staff within the business unit. Alternatively, it may be more practical to maintain a separate system to record file movements within the business unit. One such method involves the insertion of a card inside the file, on the left-hand side. The card should contain the file reference number (and part number if appropriate). When the file is removed from the registry the card should be removed, annotated with details of the member of staff to whom the file has been issued, and retained in the registry until the file is returned.

4.7.5 Whichever method is used, a system of identifying the whereabouts of files which are removed from the registry must be established, both to ensure effective file management and to satisfy security requirements.

## 4.8 Placing Documents onto Registered Files

4.8.1 Sound decisions must be taken when determining whether documents should be placed on a registered file. Not all documents generated or received by MoD business units warrant retention on file but the following definitions are helpful:

- ***Documents*** can be defined as any tangible information received or produced by MoD.
- ***Records*** can be defined as those documents that support some official activity or decision and need to be preserved for future reference
- ***Documents which are deemed to be records should be placed in the appropriate registered file.***

4.8.2 It is important to ensure that material which is deemed worthy of retention on a registered file is placed on the file as soon as possible. The registered file is the definitive record of business unit activity on any given subject and it is imperative that anyone using a file can be confident that the information it contains is complete and up-to-date.

4.8.3 Documents should be placed on the right hand side of the file and secured by an India tag to form enclosures within that file. Enclosures should be placed on the file in date of origin order (not date of receipt) and each enclosure should be sequentially numbered, e.g. **E1**, **E2** etc.

4.8.4 Annexes and attachments need not be given separate enclosure numbers provided they are referenced in the covering document. Where appropriate, annexes bearing a protective marking must be recorded in the PDR and identified by enclosure number and annex suffix.

4.8.5 Late enclosures should also be filed in date of origin order. This will mean inserting them between existing closures. Existing enclosure numbers should not be deleted and changed. Instead, the new enclosure is to be given the number of the immediately preceding enclosure followed by a sub-number. Thus if three late enclosures were to be inserted between the existing enclosures **E2** and **E3** they would be numbered **E2/1**, **E2/2** and **E2/3** respectively. The original **E2** would then be amended to reflect the number of additional enclosures which have been added in front of it, e.g. in this case **E2+3**.

4.8.6 In instances where an item is too bulky to place within the file details of the item (title; reference; date;

physical location) should be entered on the file minute sheet. When the file is closed the item is to be passed with the file to the officer responsible for review in accordance with para 4.18 below.

## 4.9 The File Minute Sheet

4.9.1 The left-hand side of the file is reserved for the file minute sheet, which should be used to record any comments about the content of the file. The minute sheet should be used to record details of significant enclosures which are being placed on the file, including those which will require the retention of the file for a specified period for administrative purposes, or those which appear to have historical value which will merit a recommendation that the file be passed to Defence Records. Each minute should be numbered and the classification of the minute should be indicated.

4.9.2 When a file is being passed to a colleague for action a covering minute can be placed on the minute sheet. When this is done the minute or enclosure number should be entered on the front cover of the file along with the title of the person to whom the file is being referred. An example of a minute sheet is at Annex C.

## 4.10 Record of Classified Documents (TOP SECRET and SECRET)

4.10.1 When an enclosure classified SECRET or above is placed on a file its existence and enclosure number is to be recorded on **MOD Form 672 -** "Record of Classified Documents (TOP SECRET and SECRET)" which is to be placed on the left hand side of the file.

## 4.11 Transfer of Enclosure Between Registered Files

4.11.1 Enclosures should only be transferred between files if they have been misfiled.

4.11.2 Action to be taken on file from which enclosure is transferred

The following information should be recorded either on the file minute sheet or on a piece of paper inserted in place of the enclosure: -

- the date of removal of the enclosure
- the documents reference
- the protective marking
- the file number of the file to which it has been transferred
- the new enclosure number
- The signature of the officer authorising/making the transfer.

4.11.3 Action to be taken on file receiving enclosure

The transferred enclosure should be inserted on the new file in date of origin order. The original enclosure number should be crossed out (but not deleted) and the document annotated with the relevant new enclosure number (JSP 441, para 4.8.3, refers). A note should be added to the file minute sheet recording the following details: -

- the document's previous file reference and enclosure number
- any protective marking
- the date of transfer
- the signature of the officer authorising/making the transfer.

## 4.12 Access to Registered Files

4.12.1 Registered files may be circulated to anyone within MOD on a "need to know" basis, provided they are cleared to the appropriate level. They may also be circulated to other government departments or external legal advisers, where appropriate, and to the National Audit Office. Otherwise, files are not to be sent outside MOD without the prior approval of DG Info-Records.

4.12.2 When files are dispatched to anyone outside the business unit their destination should be recorded on the Registered File Record Sheet (**MOD Form 262A**).

4.12.3 Where necessary, and with the approval of Head of Business Unit, a file may be marked "**Not to be sent outside the business unit without the approval of .... [a named individual]**".

## 4.13 Temporary Enclosure Jackets (TEJs)

4.13.1 TEJs should be used when there is a need to consult others about papers on a registered file but it is not convenient to forward the complete file. Copies of the appropriate papers along with covering correspondence may be placed in a TEJ (**MOD Form 174**) and forwarded to the appropriate business unit. A separate Registered File Record Sheet (**MOD Form 262A**) should be raised to record the existence of the TEJ and to whom it has been sent. The TEJ should bear a protective marking appropriate to its own contents and not necessarily the marking borne by the parent file. A **MOD Form 672** should be used where appropriate (see para 4.10.1). The TEJ should bear the file reference and title of the parent file with the addition of its own TEJ number, e.g. **TEJ NO 1** and so on.

4.13.2 The TEJ must be returned to the originating business unit for incorporation into the parent file as soon as possible. It should be placed in the file in date order (according to the date returned which should be marked on the TEJ cover), and allocated an enclosure number. The file minute sheet should be annotated to record the enclosure number of the TEJ along with details of the number of enclosures contained within it. The TEJ Registered File Record Sheet (**MOD Form 262A**) should be annotated to record the date on which the TEJ was incorporated into the file. Once the TEJ has been incorporated into the file no further enclosures are to be added to it.

## 4.14 Upgrading of Registered Files

4.14.1 MOD uses a system of colour coded file covers to denote the highest classification of the content. The following file covers are available:

- **Top Secret (Red) - MOD Form 329A**;
- **Secret (Pink) - MOD Form 329B**;
- **Confidential (Green) - MOD Form 329C**;
- **Restricted/Unclassified (Brown) - MOD Form329D**.

4.14.2 A registered file must not be opened until there is an enclosure to be placed on it. The classification of the enclosure will determine the file cover to be used. File cover denoting a classification higher than the first enclosure(s) are not to be used in anticipation of material which might be placed on the file later.

4.14.3 It will sometimes be necessary to upgrade a file to reflect the fact that a new enclosure is of a higher classification than the existing file. When this is the case, a new file cover should be produced and given an identical number to the old cover. The contents of the old file should be removed and transferred to the new cover along with the top half of the front of the old cover which should be placed in the new file on the left hand side.

**See Figure 4.2 - Example of Upgraded File Cover**

4.14.4 The date of opening of the original file should be entered on the front cover of the upgraded file (e.g.

not the date on which the file was upgraded). The date on which the file was upgraded should be entered beneath the date of opening, as in the example overleaf. The File Record Sheet (**MOD Form 262A**) must also be amended to show the date of upgrading, along with the new protective marking.

4.14.5 If there is a subsequent need to upgrade the file again then the above action should be repeated. The top half of each pre-existing file cover should be retained in the new file.

4.14.6 Remember that if a file is upgraded to SECRET a **MOD Form 672**, "Record of Classified Documents (TOP SECRET and SECRET)", will need to be raised and inserted in the file on the left-hand side.

## 4.15 Transfer of Files to Another MOD Business Unit or to Another Government Department

4.15.1 From time to time the need may arise to transfer a file or a series of files to another MOD business unit, for instance when a reorganisation results in the transfer of responsibility for a particular project to a different business unit.

4.15.2 When such a need arises as the result of, say, an entire business unit being transferred to another directorate, it may be possible to retain the existing file numbers and amend the business unit title on the file covers, which is permissible. DR3 should be advised in writing if such action is taken. However, it may not be practical to retain the existing file number (e.g. in cases where the existing number duplicates a number already used by the "importing" business unit) in which case the existing files will need to be closed and new files opened by the "importing" business unit which can then allocate new file numbers. In no circumstances may a file be renumbered. If there is a need to allocate a new number the file must be closed and a new file opened. The files should then be cross-referenced.

4.15.3 In most circumstances, if parts of a file series are being permanently transferred to a new business unit the relevant files should be closed and forwarded to the "importing" business unit which will open appropriate files, allocate new file reference numbers, and raise new Registered File Record Sheets (**MOD Form 262A**).

4.15.4 In either case, the appropriate MOD Form 262As must accompany the transferred files to the "importing" business unit where they should be attached to the new MOD Form 262As. The "exporting" business unit must formally record the transfer of the files in the File List and may, additionally, retain a copy of the relevant MOD Form 262As annotated to record the transfer. The "exporting" business unit must also notify DG Info-Records3 of the transfer.

4.15.5 Where the exporting business unit retains previous (closed) parts of the file they should also be forwarded to the importing business unit. Additionally, any Registered File Disposal Forms **(MOD Form 262F**s) held for previous parts of the file should be forwarded.

4.15.6 In cases of doubt as to the appropriate way to proceed, please contact DR3 for advice.

4.15.7 If the need arises to transfer a file permanently to another government department (e.g. on a transfer of function) DG Info-Records3 must be consulted before any transfer action is taken.

## 4.16 Missing Files

4.16.1 If, after a thorough search, a registered file cannot be located, a written report is to be submitted to DG Info-Records3. The report is to identify the file concerned, its protective marking, and the nature of its contents and is to contain an explanation of the circumstances surrounding its loss. If the file contained classified information a report is also to be submitted to the appropriate security directorate in accordance with the instructions in JSP 440.

## 4.17 Closure of Registered Files

4.17.1 There are a number of factors which need to be assessed when determining whether to close a file. The age of the file, its size and the frequency of use all need to be taken into account. If any of the following criteria apply the file should be closed:

- the file is 1 inch thick;
- the file contains 100 enclosures;
- the file has been open for 5 years;
- nothing has been added to the file for the last year (close the file unless there is a clear indication that papers will be added to it shortly);
- action on the subject covered by the file has come to an end.

## 4.18 Action to Take When Closing a Registered File

4.18.1 There are a number of actions to be taken when closing a registered file:

- mark the file boldly on the front cover "**CLOSED - NO NEW PAPERS TO BE PLACED ON THIS FILE**";
- note the date of closure on the MOD Form 262A along with the date of the last enclosure on the file (boxes are provided on the form for both dates).
- raise a Registered File Disposal Form (**MOD Form 262F**). The file title, file reference, part number, and protective marking (where applicable) should be entered on the form along with the date of the last enclosure and the date of closure of the file. Section I of the form should then be completed. This records the Disposal Schedule recommendation (see Chapter 5, paras 5.3 and 5.4). An example of **MOD Form 262F** is at Chapter 5, Annex C;
- check the file minute sheet to see whether the file contents include any items which, because of their bulk, could not be placed within the file (para 4.8 refers). If so then ensure that these items are retrieved and associated with the file before it is passed to the relevant desk officer for review.
- insert the **MOD Form 262F**, completed as above, onto the file on the right hand side, (e.g. on top of the last enclosure);
- pass the file to the desk officer responsible for reviewing it and completing sections 2 and 3 of the **262F** in line with the instructions concerning file review at Chapter 5, para 5.5.
- when the file is returned by the desk officer action should be taken in accordance with the instructions on the **262F**. If the file is to be retained locally for a period of time prior to destruction or passage to DG Info-Records a **B/F** (bring/forward) date should be recorded and the file should be put away, in the correct numerical order, with the other closed records held by the business unit.

[Note that closed files should be kept separately from open files.]

## 4.19 "Weeding" of Registered Files

4.19.1 The term "weeding" may be interpreted in different ways. However, it is defined in this manual as the removal of enclosures from a registered file for the purpose of destroying them.

4.19.2 The weeding of registered files has, in the past, been expressly forbidden under MOD rules. One of the reasons for this is that the Public Record Office (PRO) requires MOD to select complete files for permanent preservation rather than extracts from files. This is to ensure that preserved documents retain their original context. Additionally, the process of weeding files is a time-consuming and therefore costly activity.

4.19.3 With the advent of the Disposal Schedule (see Chapter 5, para 5.3) files which appear to merit consideration by DG Info-Records for permanent preservation should, where possible, be identified and marked accordingly on the schedule. Files which are so identified must not be weeded.

4.19.4 At the discretion of the Head of Business Unit, files which are identified in the Disposal Schedule as suitable for local destruction may be weeded (subject to the limitations identified at Annex D to this chapter and in accordance with locally issued instructions which incorporate the requirements outlined in that Annex).

4.19.5 In deciding whether to issue local instructions allowing the weeding of files which are to be destroyed locally Heads of Business Unit should take the following factors into account:

- the process of weeding files is a time-consuming activity, invariably involving desk officers in determining which enclosures can be removed as well as registry staff and the desk officer in recording the action taken;
- the weeding of a file will lead to a problem if a decision is taken subsequently that the file may, after all, merit consideration for permanent preservation. This might occur if events result in a subject taking on an importance which was not previously apparent. While the Disposal Schedule can be amended to record the change of status, missing enclosures will render it difficult to submit the file to the PRO for permanent preservation;
- there is a real risk that files which merit permanent preservation will be inadvertently weeded;
- though the removal of enclosures which are no longer needed may render a file more manageable, the timely closure and review of files and the opening of new parts where necessary, is a more cost-effective option.

For these reasons it is recommended that Heads of Business Unit do not authorise the weeding of registered files**. It should also be noted that no such authority can be issued in the absence of a Disposal Schedule**.

## 4.20 Procedures to be Followed if Weeding a File

4.20.1 The procedures to be followed if the weeding of files is to take place are outlined at Annex D of this chapter.

## 4.21 Records Not Placed in Registered Files

4.21.1 Not all records will be placed in registered files. Records may be in a range of other forms such as maps, plans, drawings, charts, video, film, photographs etc. Additionally, an increasing amount of material may now be stored in electronic form. The treatment of information held in electronic form is dealt with in Chapter 6. Other types of material, though they may not take the form of conventional registered files, should be assessed in the same way to determine what ongoing administrative or historical value they may have. If the material is deemed to have possible historical value rendering it worthy of consideration for permanent preservation it should be forwarded to DG Info-Records in accordance with the instructions in Chapter 5.

4.21.2 A 'Record of Unregistered Material" should be established, identifying the nature and form of such material. Such a record should be held alongside the business unit file list

4.21.3 Other records which are not on registered files might also exist, for instance groups of papers held by desk officers, perhaps containing copies of papers placed on registered files and/or copies of drafts, rough notes etc. There is unlikely to be a definitive list of such material and the responsibility for its safekeeping and disposal, in accordance with security regulations, will rest with the officers holding the information. It is important, however, to ensure that material which ought to be placed on the relevant registered file is not retained by individual officers instead.

## 4.22 Scientific and Technical Reports

4.22.1 Scientific and technical reports represent an important source of material for the Public Record Office. The most practical way of preserving a record of scientific and technical developments made by MOD establishments is to retain, where possible, complete sets of formal papers and similar documents for submission to DG Info-Records in accordance with the instructions in Chapter 8.

## 4.23 Cessation of the Use of the Designation "Not For NAO Eyes"

4.23.1 Prior to 17 July 1997 the designation "Not For NAO Eyes" was used to identify material which related to interaction with the National Audit Office (NAO) and the Public Accounts Committee. Such material was placed on files bearing distinctive numbers in the 9000 series.

4.23.2 DCI Gen 207/97 announced the cessation of that practice and stipulated that the designation "Not For NAO Eyes" ceased to apply, with all files previously withheld from the NAO now available to them should they wish to see them. The DCI also stipulated that there was no need to trawl through old files to remove the designation individually.

4.23.3 The guidance in JSP 414, Part IV, Chapter 5, Annex B has accordingly been superseded and will be amended in due course. Any enquiries related to this policy change should be addressed to G F Policy 2 on 84576MB.

4.23.4 All files in the 9000 series should now have been closed. Papers which would previously have been placed in these files should now be placed in an alternative file.

Home Back to Contents Top of Page Chapter 5 Index

Last updated 03/04/03

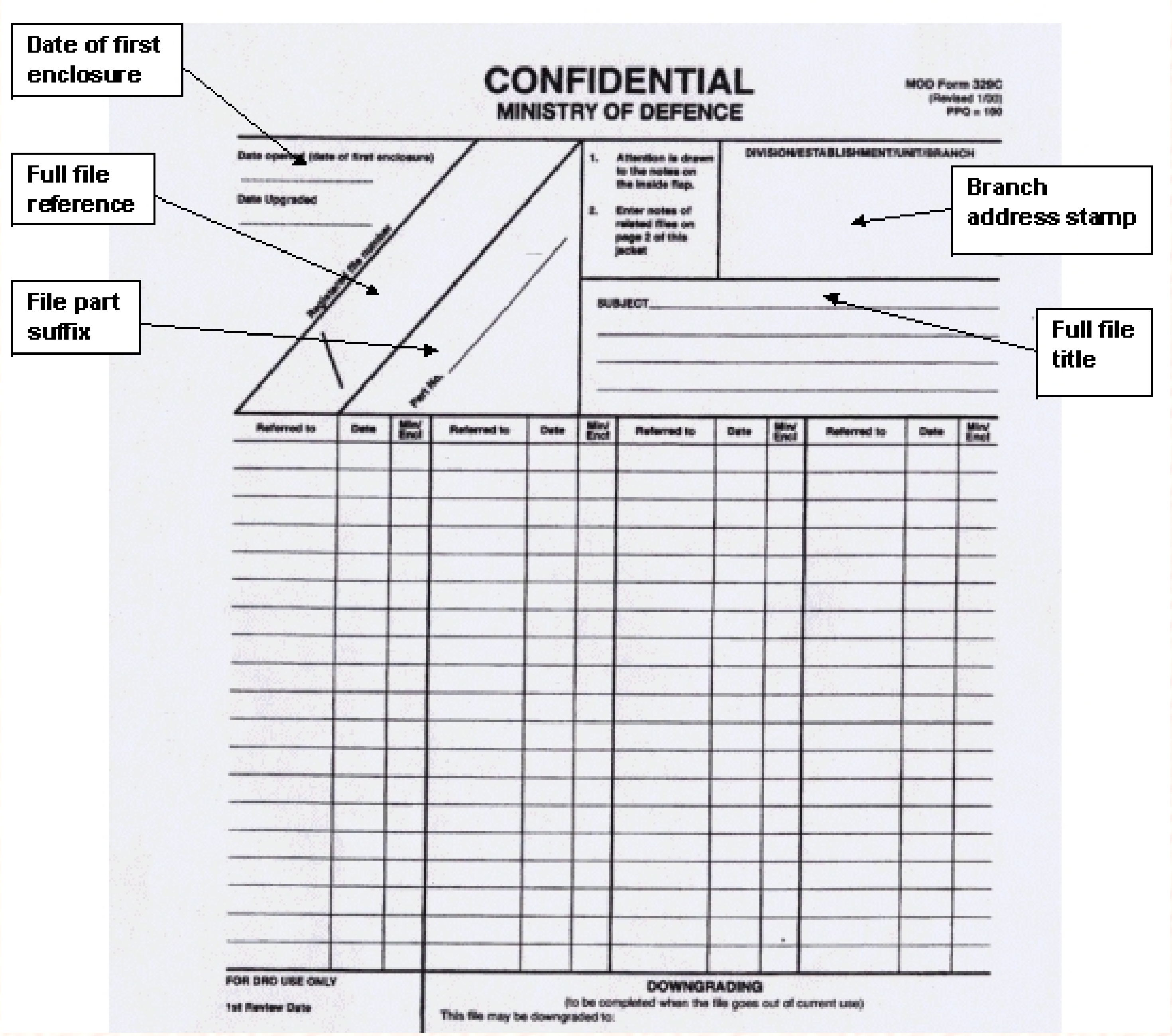
This Page Last Updated: Monday, 11 March 2002 11:50

Queries, Suggestions, etc.

# JSP 441 Defence Records Management Manual Chapter 4 Annex A

# Example of a Completed Registered File Cover

### Figure 4A.1 - Registered File Cover



Date of first enclosure

Full file reference

File part suffix

Branch address stamp

Full file title

**CONFIDENTIAL**
**MINISTRY OF DEFENCE**

MOD Form 329C
(Revised 1/00)
PPQ = 100

Date opened (date of first enclosure) ____________

Date Upgraded ____________

Registered file number

Part No. ____________

1. Attention is drawn to the notes on the inside flap.
2. Enter notes of related files on page 2 of this jacket

DIVISION/ESTABLISHMENT/UNIT/BRANCH

SUBJECT ____________

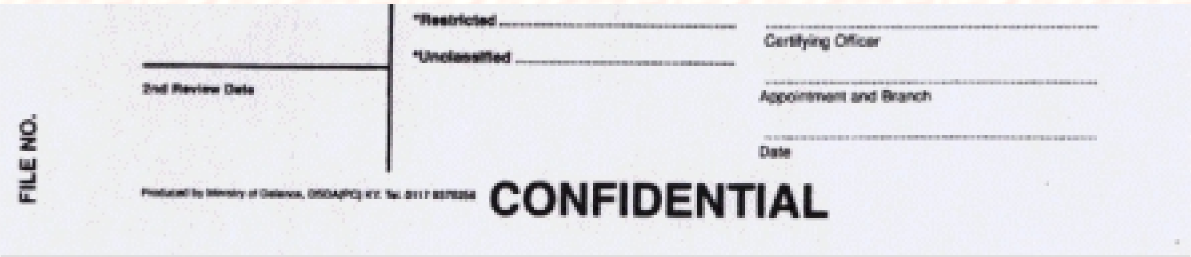
| Referred to | Date | Min/ Encl | Referred to | Date | Min/ Encl | Referred to | Date | Min/ Encl | Referred to | Date | Min/ Encl |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

FOR DRO USE ONLY

1st Review Date

**DOWNGRADING**
(to be completed when the file goes out of current use)

This file may be downgraded to:



FILE NO.

2nd Review Date

*Restricted ..........................................

*Unclassified ..........................................

..........................................

Certifying Officer

..........................................

Appointment and Branch

..........................................

Date

Produced by Ministry of Defence, DSDA(PC) KY. Tel. 0117 [illegible] CONFIDENTIAL

**(i)** The above example indicates the information which should be recorded on a registered file cover. Note that the "Date Opened" should correspond to the date of the first enclosure placed on the file (see para 4.6.1).

**(ii)** Note that the "Part Reference" should only be completed if a subsequent part to a file is opened, i.e. once Part B is opened the cover of the pre-existing file should be amended to indicate that it is now Part A (see para 4.6.2).

Home Page Back to Contents Back to Chapter 4 Top of Page Index

This Page Last Updated: Thursday, 03 April 2003 10:45

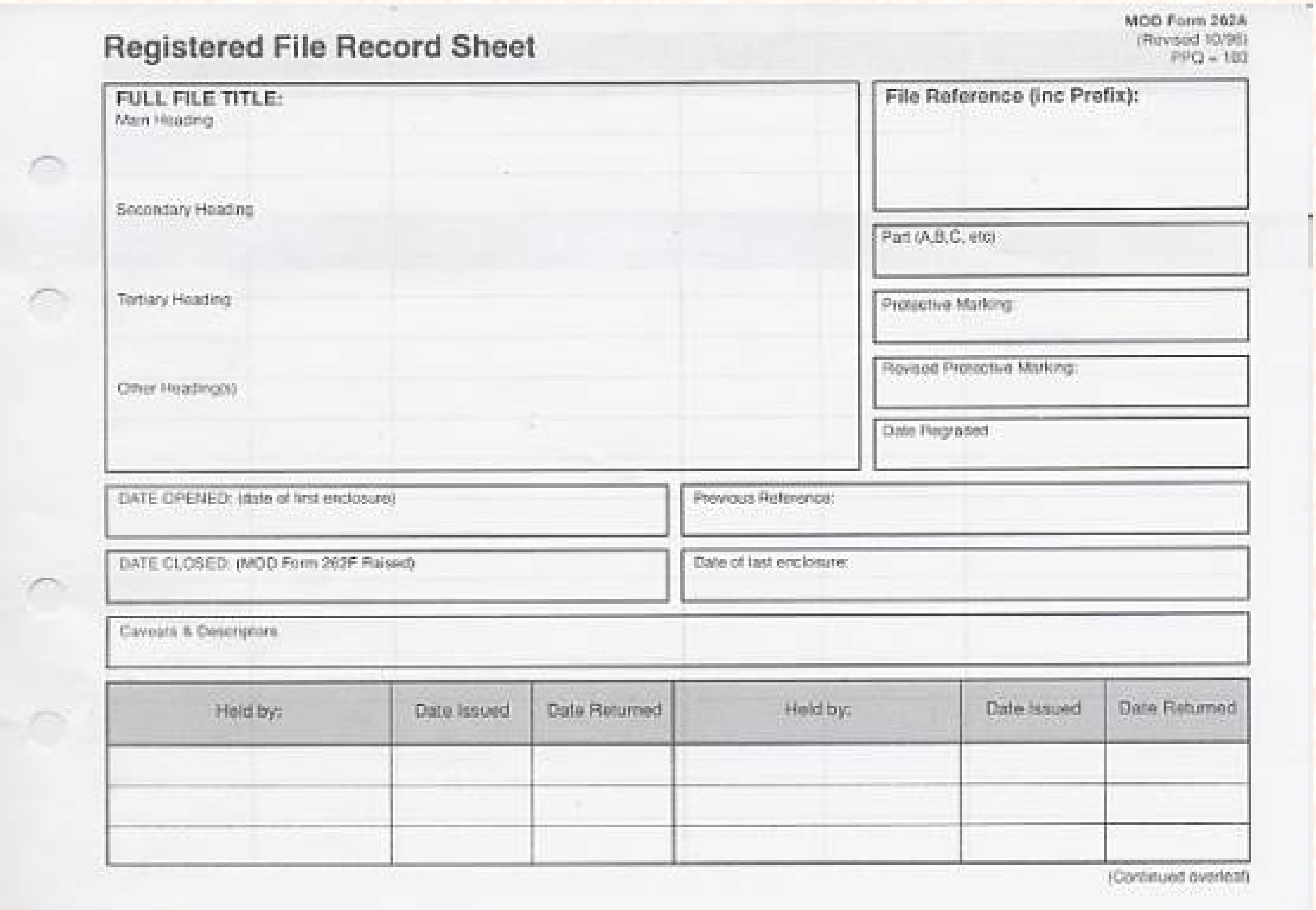
Queries, Suggestions, etc.

**JSP 441**

**Defence Records Management Manual Chapter 4 Annex B**

# Example of a Registered File Record Sheet (MOD Form 262A)

**Figure 4B.1 - Registered File Record Sheet (front and back)**



MOD Form 262A
(Revised 10/98)
PPQ - 100

## Registered File Record Sheet

**FULL FILE TITLE:**

Main Heading

Secondary Heading

Tertiary Heading

Other Heading(s)

**File Reference (inc Prefix):**

Part (A,B,C, etc)

Protective Marking:

Revised Protective Marking:

Date Regraded

DATE OPENED: (date of first enclosure)

Previous Reference:

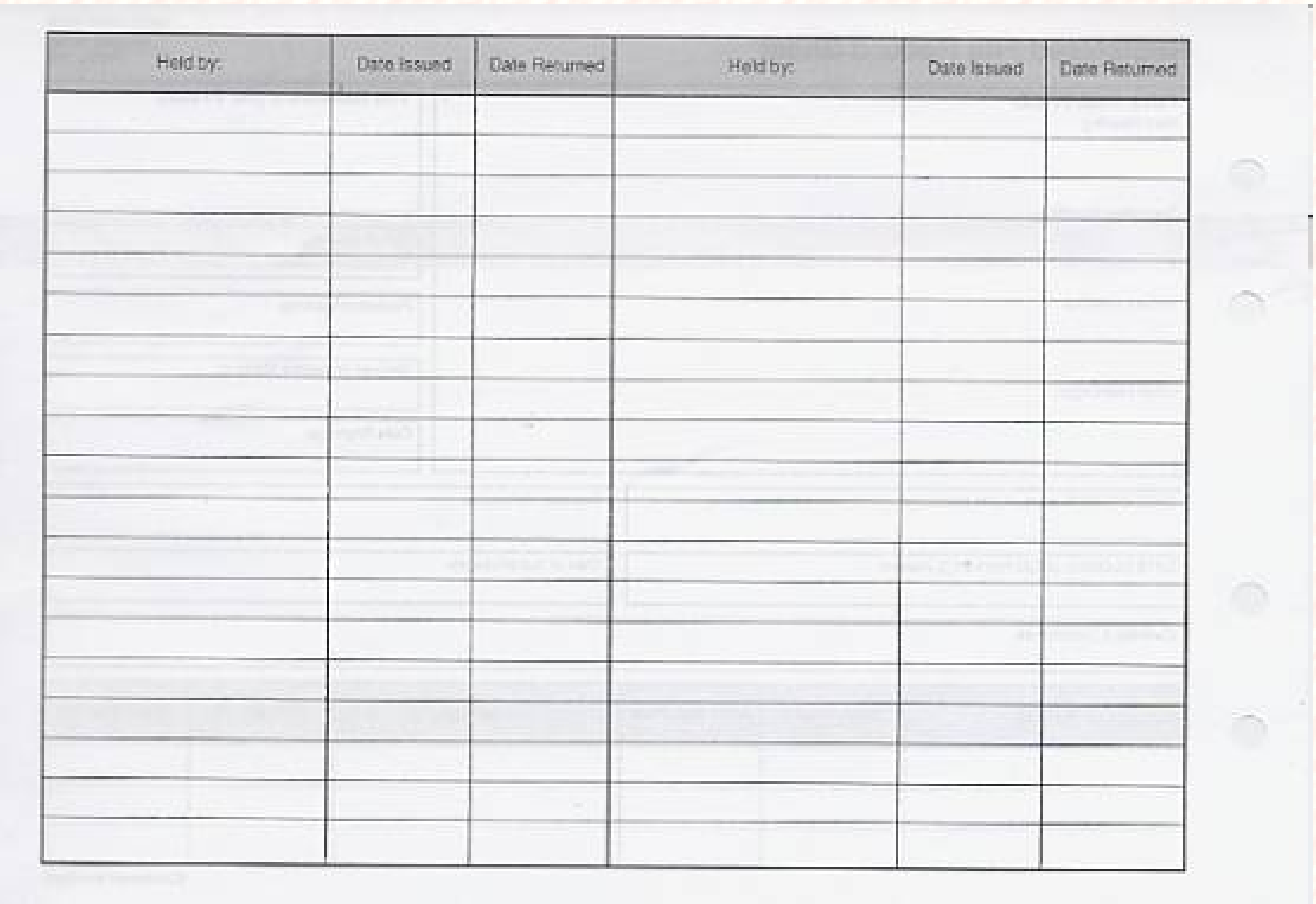
DATE CLOSED: (MOD Form 262F Raised)

Date of last enclosure:

Caveats & Descriptors

| Held by: | Date Issued | Date Returned | Held by: | Date Issued | Date Returned |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

(Continued overleaf)



| Held by: | Date Issued | Date Returned | Held by: | Date Issued | Date Returned |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**(i)** A MOD Form 262A must be raised whenever a new registered file or a subsequent part to an existing file is opened. The 262A is the definitive record of the files existence.

**(ii)** When a registered file is closed the date of closure is to be recorded on the MOD Form 262A along with the date of the last enclosure on the file (boxes are provided on the form for both dates).

**(iii)** 262As are to be placed in suitable binders (MOD Form 262 is provided for the purpose) and maintained until replaced by a Registered File Disposal Form (MOD Form 262F). Guidelines on the use of MOD Form 262F are at para 4.18.

**(iv)** Ensure that the information on the form concerning the Protective Marking allocated to the file is kept up to date and includes details of any regrading.

**(v)** If a registered file is sent temporarily to another business unit the details must be recorded on the 262A, including the date sent and the date returned.

**(vi)** The 262A may also be used to record that a file has been issued to a member of staff within the business unit. If it is not, a locally devised system must be used (see para 4.7.4).

**(vii)** If a registered file is transferred permanently to another business unit the 262A must accompany it. A copy of the 262A may be retained annotated to record the transfer (see para 4.15.4).

Home Back to Contents Back to Chapter 4 Top of Page Index

Last updated 03/04/03

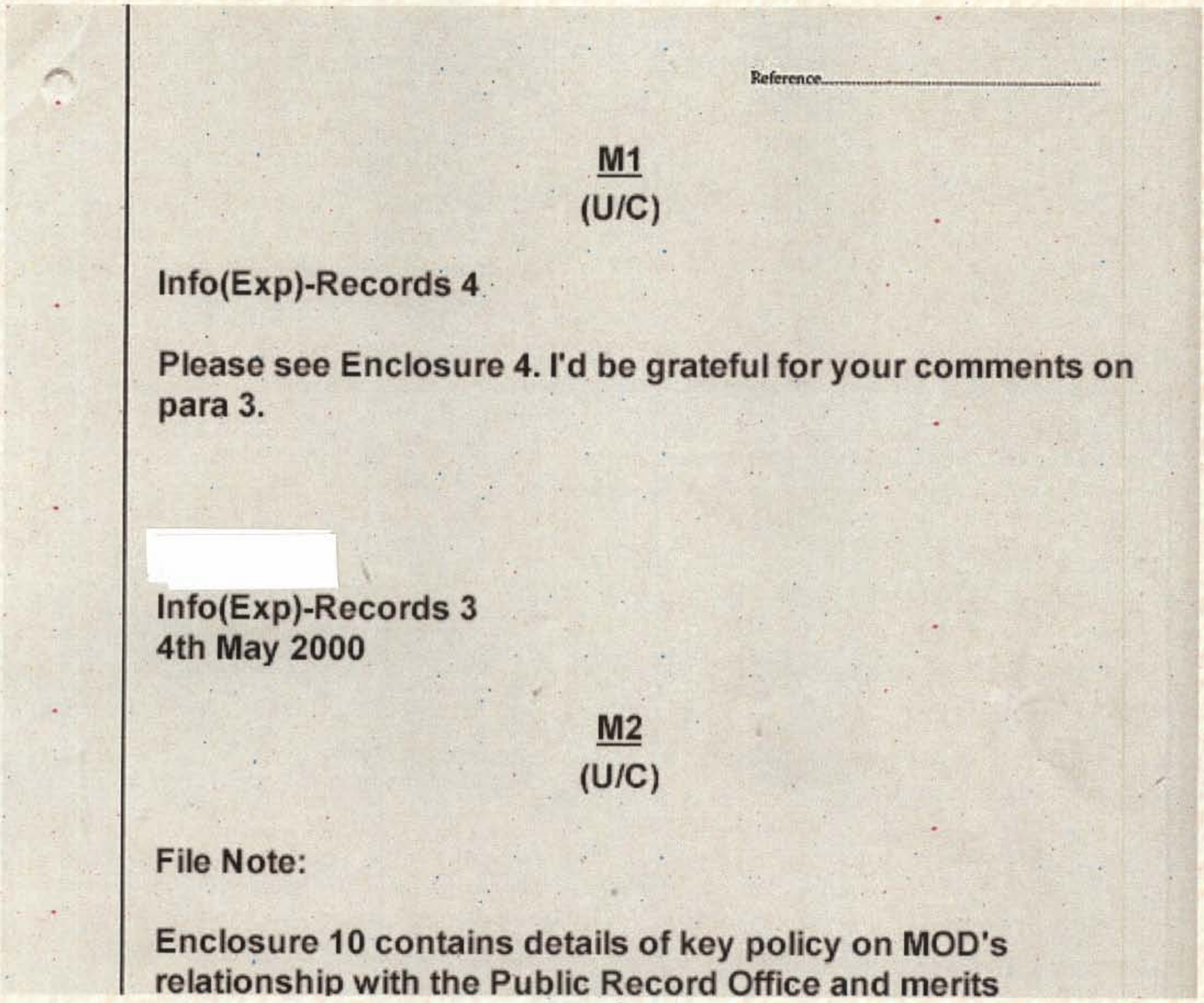
This Page Last Updated: Monday, 11 March 2002 11:54

Queries, Suggestions, etc.

**JSP 441** **Defence Records Management Manual Chapter 4 Annex C**

# Example of a Completed Registered File Minute Sheet

**Figure 4C.1 - File Minute Sheet**



Reference.........................................

**M1**

**(U/C)**

Info(Exp)-Records 4

Please see Enclosure 4. I'd be grateful for your comments on para 3.

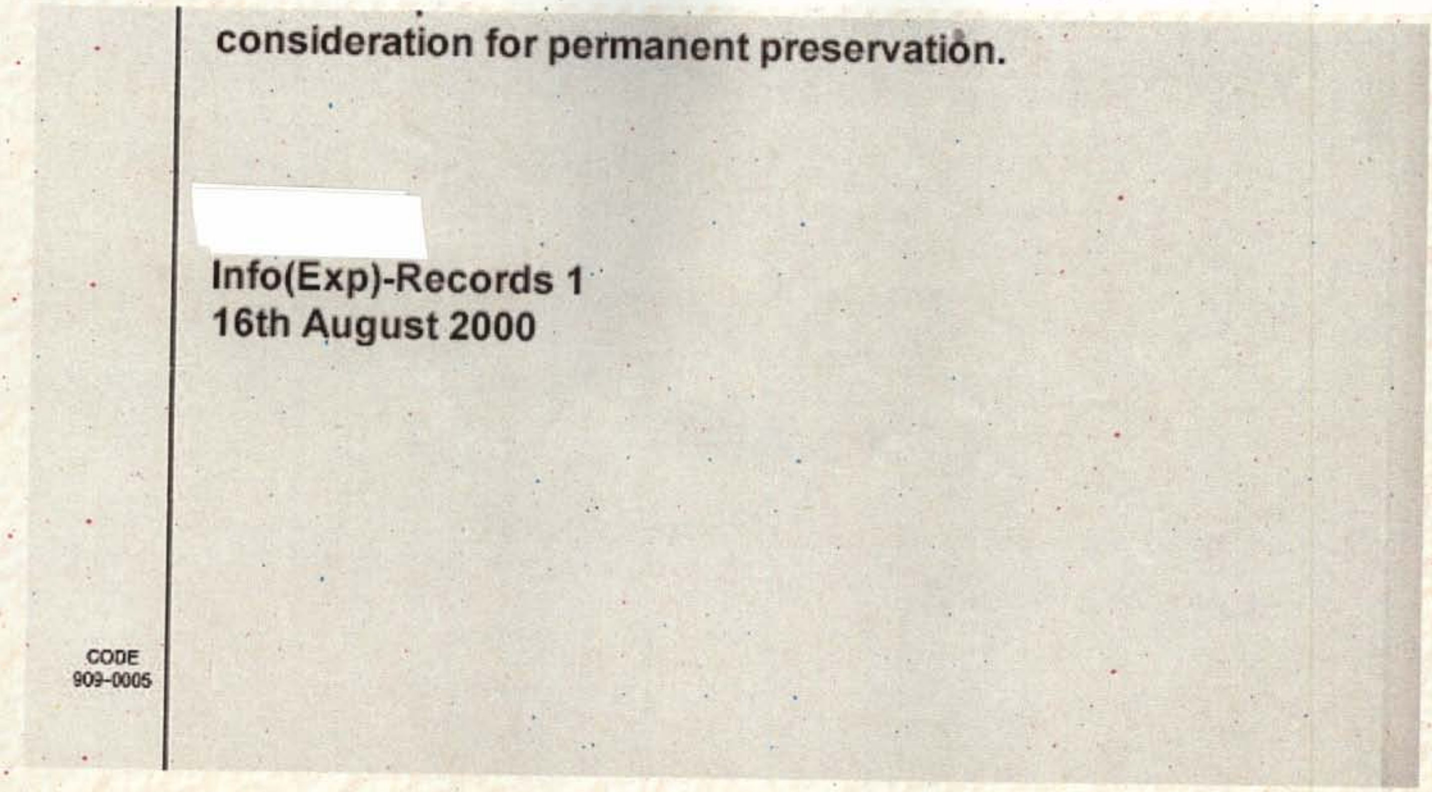
Info(Exp)-Records 3
4th May 2000

**M2**

**(U/C)**

File Note:

Enclosure 10 contains details of key policy on MOD's relationship with the Public Record Office and merits



consideration for permanent preservation.

[redacted]

Info(Exp)-Records 1
16th August 2000

CODE
909-0005

(i) Above is an example of a registered file minute sheet. Minute 1 is a note from Info(Exp)Records3 to a colleague drawing his attention to a specific enclosure on the file and requesting comments regarding a particular issue which has been raised.

(ii) Minute 2 is a note made by Info(Exp)Records1 which identifies a particular enclosure as containing key policy and therefore likely to render the file worthy of consideration for permanent preservation. The use of the minute sheet to record this fact ensures that when the file is closed and reviewed in line with the instructions in Chapter 5, para 5.5, the officer conducting the review will be able to readily see that the file may merit permanent preservation, and will be alerted to this particular key enclosure.

(iii) Note that both minutes have been identified as Unclassified.

(iv) Note that the file reference number has been included at the top right hand corner of the page. This is a useful precaution in case the minute sheet should inadvertently become detached from the file.

(v) Further information on the use of the file minute sheet is at para 4.9.

Home Back to Contents Back to Chapter 4 Top of Page Index

Last updated 11/03/02

This Page Last Updated: Monday, 20 January 2003 11:30

Queries, Suggestions, etc.

JSP 441

Defence Records Management Manual Chapter 4 Annex D

# Rules Governing the Weeding of Registered Files

(i) If the weeding of registered files is to be authorised the front covers of all files listed in the business unit Disposal Schedule as worthy of consideration by DG Info-Records for permanent preservation must be annotated with a **MOD Form 494**, "Do not Weed" notice.

(ii) It should be noted that in addition to files marked for permanent preservation all files containing TOP SECRET and Codeword material are to be forwarded to DG Info-Records, even if the accompanying recommendation is that the file can be destroyed. These files are not to be weeded.

(iii) Files containing ATOMIC and Nuclear records worthy of consideration for permanent preservation must be forwarded to DG Info-Records in accordance with the instructions in Chapter 8 and are not to be weeded. (Files containing such material which are not identified as requiring permanent preservation should be maintained in accordance with **ACO 130**, "Rules for Handling, Protection and Release of Information Marked Atomic").

(iv) Where no decision about a file's disposal has been recorded in the Disposal Schedule the file must not be weeded.

**(v) MOD Form 494 must be placed on the front cover of all of the files identified above,**

(vi) A record must be maintained within each weeded file to identify which enclosures have been removed. This is necessary in order to satisfy both security and audit requirements. The following information is to be recorded:

-
- the relevant enclosure number;
- the document reference number and date of origin;
- the protective marking of the document;
- confirmation that the document has been removed for destruction;
- the authorising officer's signature and the date of removal

(vii) The record of removal may be maintained on a locally devised form inserted inside the file cover on the left hand side or, alternatively, on an individual sheet inserted in place of the document removed and allocated the enclosure number of that document. The maintenance of such a record does not negate the need to fully comply with the instructions in **JSP 440** governing the destruction of classified material.

Home Back to Contents Back to Chapter 4 Top of Page Index

Last updated 20/01/03

**This Page Last Updated:**
**Thursday, 03 April 2003 12:31**

Queries, Suggestions, etc.

**JSP 441**

**Defence Records Management Manual Chapter 5**

# Review of Records Held by Business Units

## 5.1 The Role of the Departmental Records Officer

5.1.1 In some government departments the ultimate decision about destroying records held in registered files is made centrally by the staff of the Departmental Records Officer. Within MOD Head of DG Info-Records, who is the DRO, has delegated authority to business units to review the records they hold and, in most cases, destroy locally those records which are not considered worthy of permanent preservation. This can be done when the records cease to have administrative value.

5.1.2 The exception to this rule is that all registered files containing TOP SECRET and Codeword material are to be forwarded to DG Info-Records and are not to be destroyed locally, though the recommendation to DG Info-Records may be that they can be destroyed.

5.1.3 All other registered files (and unregistered records) which are identified by the business unit as meriting consideration for permanent preservation are to be sent to DG Info-Records in accordance with the instructions in Chapter 8. Certain Air Force department files may initially be sent to the Air Historical Branch (RAF) with the prior agreement of both the AHB and DG Info-Records1. Once received they will be reviewed centrally to determine whether permanent preservation is warranted.

5.1.4 DG Info-Records conducts two reviews of registered files, the first 5 years after the closure of the file (or within a short time of its receipt if it has been kept by the business unit for a longer period). Files which do not merit permanent preservation are marked for destruction, either straight away or at a predetermined point in the future, taking into account the recommendation made by the originating business unit.

5.1.5 Those files which appear to merit permanent preservation are reviewed again some 20 years later. The second review allows a judgement to be made about the historical context of the records. Files which are selected for permanent preservation are normally passed to the Public Record Office 30 years after their closure and are then made available to the public in line with the terms of the Public Records Act of 1967.

5.1.6 Records which are not held in registered files are normally reviewed by DG Info-Records 5 years and (where applicable) 25 years after their creation

## 5.2 The Role of the Business Unit Holding the Records

5.2.1 Delegated authority allows each business unit greater flexibility to manage their records efficiently but confers a responsibility upon them to review the records they hold and dispose of them in an appropriate and timely manner.

5.2.2 This chapter outlines the procedures to be followed by business units to ensure that an effective system of review is maintained allowing those records which are no longer needed, and do not merit permanent preservation, to be destroyed, while records which are needed for administrative purposes are kept for the appropriate period and those which appear to merit permanent preservation are forwarded to DG Info-Records.

5.2.3 In reviewing the records which they hold, each business unit should consider the appropriate length of time that a file, or any other type of record, is likely to be needed for administrative purposes.

5.2.4 Having made that decision, the business unit is also well placed to make an initial judgement about the likely historical value of a file (or other type of record). To aid the business unit in making that judgement Annex A to this chapter contains guidelines on the type of records likely to merit permanent preservation. In assessing whether a file meets these criteria remember that it is the responsibility of the lead business unit to identify such files and forward them to DG Info-Records. If your file merely contains copies of correspondence relating to a topic for which another business unit has lead responsibility the file need not be forwarded to DG Info-Records.

5.2.5 There is also a need to consider whether classified material generated by the business unit which is to be retained for administrative or historical reasons continues to merit its original protective marking, or whether it should be downgraded.

5.2.6 Records which are held in electronic form are no less worthy of consideration than records held on paper. This issue is addressed in Chapter 6 - Electronic Records Management Systems.

5.2.7 In order to facilitate the review of records each business unit must establish a ***Disposal Schedule***. The procedure to be followed is outlined below.

## 5.3 The Disposal Schedule

5.3.1 The registered files (or other types of record) held by a business unit will often span a wide variety of subjects. While some may deal with matters of major significance, others will deal with more routine matters.

5.3.2 The Disposal Schedule will help each business unit to identify, where possible, an appropriate length of time for which each file (or other type of record) should be kept and how it should ultimately be disposed of. Disposal may be to DG Info-Records with a recommendation that the file warrants permanent preservation, or it may be through local destruction.

5.3.3 As most records held by a business unit should be on registered files the ***File List*** (see Chapter 4, para 4.2) should be the basis of the  Disposal Schedule.

5.3.4 Each file will contain records which fall into one of the following categories:

- records which merit consideration by DG Info-Records for permanent preservation;
- records which though not worthy of permanent preservation will need to be kept for an extended period for administrative purposes (perhaps for legal or contractual purposes);
- records which have only short term value and will not need to be retained for a lengthy period.

5.3.5 Where a file contains records which fall into more than one category it must be treated in accordance with the most important category.

5.3.6 Establishing a Disposal Schedule involves considering the existing open files held by the business unit and identifying, where possible, the category each file (or group of files) falls into. Having done that, a recommendation can then be made about the file's disposal.

5.3.7 The different types of information held within any particular business unit might include:

· Administrative Records – These records are produced in large volumes.  Generally they have low retention values and are usually disposed of within 1 to 7 years after the date of creation.

· Case Records – The retention periods for these records are usually defined by an individuals age and life span unless a statutory or a long-term operational requirement defines a period for their continued retention.  For example, records relating to criminal cases may be retained for 75 years or more.

· Command and Control and Operational Records – Some records in these categories can have a long life span and should, in many cases, be considered for permanent preservation.

· Estates and Accommodation Records – These records include a substantial amount of administrative type records with a low retention value, however certain records may be retained for much longer periods. For example:

o Legal records – estate title, leasehold documentation, etc., should be retained for at least the occupancy period.

o Policy records – surveys, policy studies etc., retention varies between 10 to 25 years but there may be records relating to important aspects such as disposal of potentially hazardous substances on sites or other health and safety issues that should be kept for much longer periods of time.

· Finance Records – These records normally have a short working life of about two years. Generally there is no legal requirement to retain these records beyond seven years.

· Health and Safety Records – As well as some statutory requirements that need to be complied with, there are those records that can have a very long retention requirement. Especially in cases involving exposure to radiation or contamination where the safety implications as a result of the contamination may only arise decades after the initial event. A retention period of up to 100 years may be required in these cases.

· Personnel Records – The retention periods for these records may vary but some should be kept for very long periods. Examples include:

o Documents that have a bearing on pension entitlement should be kept for up to 100 years from date of birth.

o Military Service personnel appraisal reports are to be kept for 100 years.

o Civilian Staff appraisal records are normally kept as separate sub-sets of personal files. If kept in annual sets, they should be destroyed on a rolling basis.

o Medical records are normally filed as a separate sub-set of individual personal files to allow for separate retention. In some instances where they relate to, for example, exposure to radiation, these may be kept for up to 100 years.

· Policy Records – These are normally retained for at least 25 years, and in cases where the records relate to the development of primary legislation, may be marked for permanent preservation.

· Scientific, Technical and Research Records – Records of the more important aspects of scientific, technological or medical research and development are normally retained as a long term research resource for other scientific researchers. Retention periods may differ, as some business units may retain these records as part of their permanent library, whilst others may consider them as case files and dispense with them after 10 years. Reports for these types of records are normally preserved, whilst the supporting information is not, however their administrative value could be long, i.e. Porton Down and paper records covering the volunteer programme go back to the 1950's.

· Transaction Records – These records record specific events that have a finite life, i.e. the award of a contract allocated to a named contractor to commission a particular task. Depending on the nature of the transaction, the retention period may vary between 6 to 25 years.

5.3.8 The varying management requirements for each of the types of information listed above also need to be considered. Factors to be considered include:

- Operational requirements.
- Business requirements.
- MOD corporate requirements.
- Public access requirements.
- Legal and statutory requirements.
- Human life expectancy.
- Volume of records likely to be generated.
- Sensitivity.
- Accessibility.

5.3.9 That recommendation should then be noted in the Disposal Schedule. An example of an extract of a completed Disposal Schedule is at Annex B.

5.3.10 In addition to the file list the "Record of Unregistered Material" (see Chapter 4, para 4.21.2) should also be considered and appropriate recommendations made, where possible.

5.3.11 The Branch Records Officer (see Chapter 3, para 3.2) is responsible for drawing up the Disposal Schedule. However, the task of recommending suitable retention periods for each file is best performed by the desk officers who use the files. They should be best placed to make this judgement based on their working knowledge of the nature of the file and its content. The Records Officer's role is to co-ordinate this task.

5.3.12 It may not be possible to make a recommendation about the disposal of every file. However, it is important to make a recommendation wherever possible. Remember that the records officer/ desk officer who will ultimately be required to make a decision about the disposal of each file may not have a detailed knowledge of the file's content because it may be up to 5 years since the file was opened and it may not have been used recently.

5.3.13 The records officer/desk officer who ultimately completes the Registered File Disposal Form (**MOD Form 262F**) may not agree with the recommendation and is free to change it. This might be necessary if subsequent events have given a different weight to the content of the file. However, where this is not the case, the recommendation can be endorsed with the confidence that it was the considered opinion of a predecessor who was familiar with the nature of the contents of the file.

5.3.14 Where it is not possible to make a recommendation about the disposal of a file the words "No Recommendation" should be entered on the Disposal Schedule. Such files are not to be weeded (see Chapter 4, Annex D, para (iv)).

## 5.4 Maintaining the Disposal Schedule

5.4.1 The recommendations noted in the Disposal Schedule will be made primarily on the basis of the type of information contained within the current part of the file. In many cases the recommendation will remain valid even when the existing file is closed and a new part opened. For instance, if a file has been recommended for passage to DG Info-Records because it illustrates significant developments in an area of policy, it is quite likely that any subsequent part of that file will fall into the same category. Equally if a file contains information which can be destroyed locally after a relatively short period this is also likely to apply to any subsequent part.

5.4.2 It may, however, be that subsequent parts of a file increase or diminish in importance in relation to previous parts. Where this is the case the desk officer should advise the records officer to amend the Disposal Schedule accordingly.

5.4.3 The revised recommendation will not necessarily mean that any previous parts of the file which were recommended for disposal in a different way were dealt with incorrectly, but see para 5.5.4.

5.4.4 The records officer is responsible for the maintenance of an up to date Disposal Schedule and the incorporation of amendments. The records officer is also responsible for ensuring that all desk officers have access to a copy of the schedule.

5.4.5 As new files (as opposed to new parts of existing files) are opened the records officer should establish whether an initial recommendation about disposal can be made. This will depend upon the nature of the file. It may be clear from the outset that the file will contain significant papers or, conversely, that the file is unlikely to contain records which will need to be retained for a lengthy period. If so a suitable recommendation can be made. If this is not possible the Disposal Schedule should be annotated to show that no recommendation has yet been made.

5.4.6 A copy of the Disposal Schedule is to be forwarded to DG Info-Records3 for reference purposes. It is not necessary to forward details of each amendment but an up to date version, or confirmation that no change has occurred, should be forwarded annually.

## 5.5 Timing of Review and Use of the Disposal Schedule

5.5.1 Chapter 4 (para 4.17) outlines the factors which determine when a registered file should be closed and the action to be taken at that time.

5.5.2 When a file is closed a Registered File Disposal Form (**MOD Form 262F**) is to be raised and placed in the file in accordance with the instructions in Chapter 4, para 4.18. At that time the Disposal Schedule is to be consulted to determine what recommendation has been made about the appropriate retention period and method of disposal. The disposal schedule recommendation should be noted in section I of the 262F and the file should then be passed to the desk officer responsible for reviewing it and completing the remainder of the form.

5.5.3 The desk officer responsible for carrying out the review must then consider the recommendation at section I of the 262F and either endorse or amend it. Before doing so the file minute sheet should be checked to see whether details of any significant enclosures have been recorded (see Chapter 4, para 4.9.1).

5.5.5 The 262F should then be completed and signed by an officer of at least HEO (or equivalent) grade (where necessary the desk officer must arrange for the form to be signed by the records officer or a line manager). If the ultimate recommendation is that the file should be retained for an extended period for administrative purposes, or that the file warrants permanent preservation, the specific enclosures which justify that recommendation (which should be identified on the file minute sheet) should be recorded on the 262F. If there are a large number of enclosures which justify such a recommendation only the key enclosures need be identified.

5.5.8 Unregistered records are to be reviewed within 4 years of their creation to determine the appropriate method of disposal. Any such records which merit consideration by DG Info-Records for permanent preservation should be forwarded in accordance with the instructions at para 5.7 and in Chapter 8.

5.5.9 An Aide Memoir outlining the review process is at Annex 5D. A diagram depicting the life-cycle of an open file is at Annex 5E and a diagram depicting the life-cycle of a closed file is at Annex 5F.

## 5.6 Existing Files Which Were Not Reviewed at Time of Closure

5.6.1 The policy governing the timing of file review was revised in August 1999 and promulgated in DCI Gen 220/99 dated 6/8/99. Prior to the introduction of the revised policy, files could be retained for up to 4 years before review and completion of the Registered File Disposal Form (MOD Form 262F). The revised policy on the timing of file review does not apply retrospectively however, consideration should be given to accelerating the review of closed files which have not yet been reviewed. **It is recommended that all such files are now reviewed, and sections 2 and 3 of MOD form 262F completed, at the earliest opportunity**.

5.6.2 With the exception of files identified at para 5.6.1 above, business units holding registered files (or unregistered records) which have not been reviewed in accordance with the instructions are para 5.5 must take remedial action to deal with the review backlog. Registered File Disposal Forms (MOD Form 262F) should be raised for these files at the earliest opportunity. The files should then be reviewed and disposed of accordingly. It is likely that many such files will have no further administrative value and will not have historical value. Such files should be destroyed locally (but see para 5.11).

## 5.7 Retention of Registered Files within the Business Unit

5.7.1 If the completed and signed Registered File Disposal Form (**MOD Form 262F**) recommends that the file should be considered by DG Info-Records for permanent preservation it should normally be sent to DG Info-Records within 5 years of its closure. Files which also have ongoing administrative value may be retained locally for an extended period and should be forwarded to DG Info-Records when they are no longer needed. **However, DG Info-Records must be advised in writing of any case in which the file is still required by the business unit for administrative purposes 25 years after closure**.

5.7.2 If the 262F recommends that the file can be destroyed locally it may be retained by the business unit for up to 25 years after its closure. **If the file has not been destroyed within 25 years of its closure permission must be sought from DG Info-Records to retain it**.

5.7.3 Files which are to be retained for an extended period for administrative purposes but which are not considered to merit permanent preservation may be forwarded to DG Info-Records for storage if there is insufficient storage space locally. In these circumstances the records officer must ensure that explicit reasons are given on the 262F for the ongoing retention of the file, in line with the instructions at paras 5.5.4 and 5.5.5. **Failure to do so may result in the file being destroyed by DG Info-Records**.

## 5.8 Retention of Other Records

5.8.1 Unregistered records which merit consideration by DG Info-Records for permanent preservation are to be forwarded within 25 years of their creation, in accordance with the instructions in Chapter 8. DG Info-Records must be advised in writing of any case in which such records are still required by the business unit for administrative purposes 25 years after closure.

5.8.2 Unregistered records required for administrative purposes may be retained by the business unit for up to 25 years after their creation. If the records have not been destroyed within 25 years permission must be sought from DG Info-Records to retain them.

5.8.3 Unregistered records which are to be retained for an extended period for administrative purposes may, by prior arrangement, be forwarded to DG Info-Records2 for storage if there is insufficient storage space within the business unit.

## 5.9 The Registered File Disposal Form (MOD Form 262F)

5.9.1 When a file is destroyed by the business unit the Registered File Disposal Form is to be removed and used to replace the Registered File Record Sheet (MOD Form 262A) which should then be destroyed.

5.9.2 If the file is not destroyed locally but is forwarded to DG Info-Records the original 262F must accompany the file. The business unit should retain a copy of the 262F, annotate it to indicate that the file has been forwarded to DG Info-Records and use it to replace the 262A which should be destroyed.

5.9.3 The Registered File Record Sheet (**MOD Form 262A**) and Registered File Disposal Form (**MOD Form 262F**) are the definitive record of a file's existence and subsequent destruction/passage to DG Info-Records. MOD Form 262A must not be destroyed until replaced by MOD Form 262F. Each 262F must be retained for a period of not less than 30 years from the date of last enclosure (as recorded on the form). As MOD Form 262Fs are normally retained in a binder relating to a file series or a number of file series the binder should normally be retained for a period of not less than 30 years following the insertion of the final 262F. If a business unit is disbanded during this period the binder(s) should pass to the successor business unit. If there is no successor business unit the binder(s) should be forwarded to DG Info-Records2 at Hayes.

5.9.4 An example of a Registered File Disposal Form and instructions on its completion are at Annex C.

## 5.10 Sponsors of Manuals and Books of Reference

5.10.1 Sponsors of books of reference, manuals, directories, etc are to ensure that a copy of the material is forwarded to DG Info-Records for consideration for permanent preservation. Sponsors are to maintain an unamended copy of each publication together with loose copies of each amendment for this purpose. Such material should be forwarded to DG Info-Records2 in accordance with the instructions in Chapter 8.

## 5.11 Destruction of Top Secret Registered Files and Files Containing Codeword Material

5.11.1 All registered files containing Top Secret and/or codeword material are to be forwarded to DG Info-Records in accordance with the instructions in Chapter 8, even if the Registered File Disposal Form recommends that the file should be destroyed.

Home Back to Contents Top of Page Chapter 6 Index

Last updated 03/04/03

**This Page Last Updated: Monday, 20 January 2003 11:56**

Queries, Suggestions, etc.

**JSP 441** **Defence Records Management Manual Chapter 5 Annex A**

# Example of Records likely to warrant Permanent Preservation

### 1. Documents/Files

- containing Top Secret or Codeword material.

### 2. Documents/Files

- containing information on important scientific/technical developments.

### 3. Documents/Files

- which have been used by Official Historians or have been marked for retention by them.

### 4. Documents/Files

- that illustrate the formation/evolution of Defence Policy or significant developments in the relationship between MOD and other organs of Government, or other national or international authorities.

  that show the authority under which MOD has exercised a function.

  that contain important decisions relating to the organisation, disposition or use of the Armed Forces

  that show the reasons for important decisions or actions or provide precedents.

  that could help the Government to establish, maintain, or control a legal claim or title

  that reflect Law Officers opinion on any subject.

### 5. Documents/Files and other records

- of the setting up, proceedings and reports of committees, working parties and study groups.

  of the introduction/consideration of new types of weapons and equipment.

  of important trials and exercises.

  of the introduction of new types of uniforms, clothing etc of the formation, organisation, reorganisation, redesignation or disbandment of units.

of notable courts martial and other legal matters.

of the occupation of historic buildings and sites of archaeological interest.

of matters of significant regional or local interest which are unlikely to be documented elsewhere.

of subjects of general national or international interest.

### 6. Reports

- of significant operations, intelligence, organisational and logistic matters.

### 7. Histories

- produced by Service units etc.

### 8. Standing Orders

- and similar instructions of Commands, Agencies, Establishments etc.

### 9. Diaries

- journals, logs etc providing an insight into particular operations or activities of wide interest

### 10 .Records

relating to famous or infamous people.

**Note:** In assessing whether a file merits passage to DG Info-Records with a recommendation that it be considered for permanent preservation it is important to remember that it is the responsibility of the lead business unit to identify and forward such files. If your file merely contains copies of correspondence relating to a topic for which another business unit has lead responsibility the file need not be forwarded to DG Info-Records.

Home Back to Contents Back to Chapter 5 Top of Page Index

Last updated 20/01/03

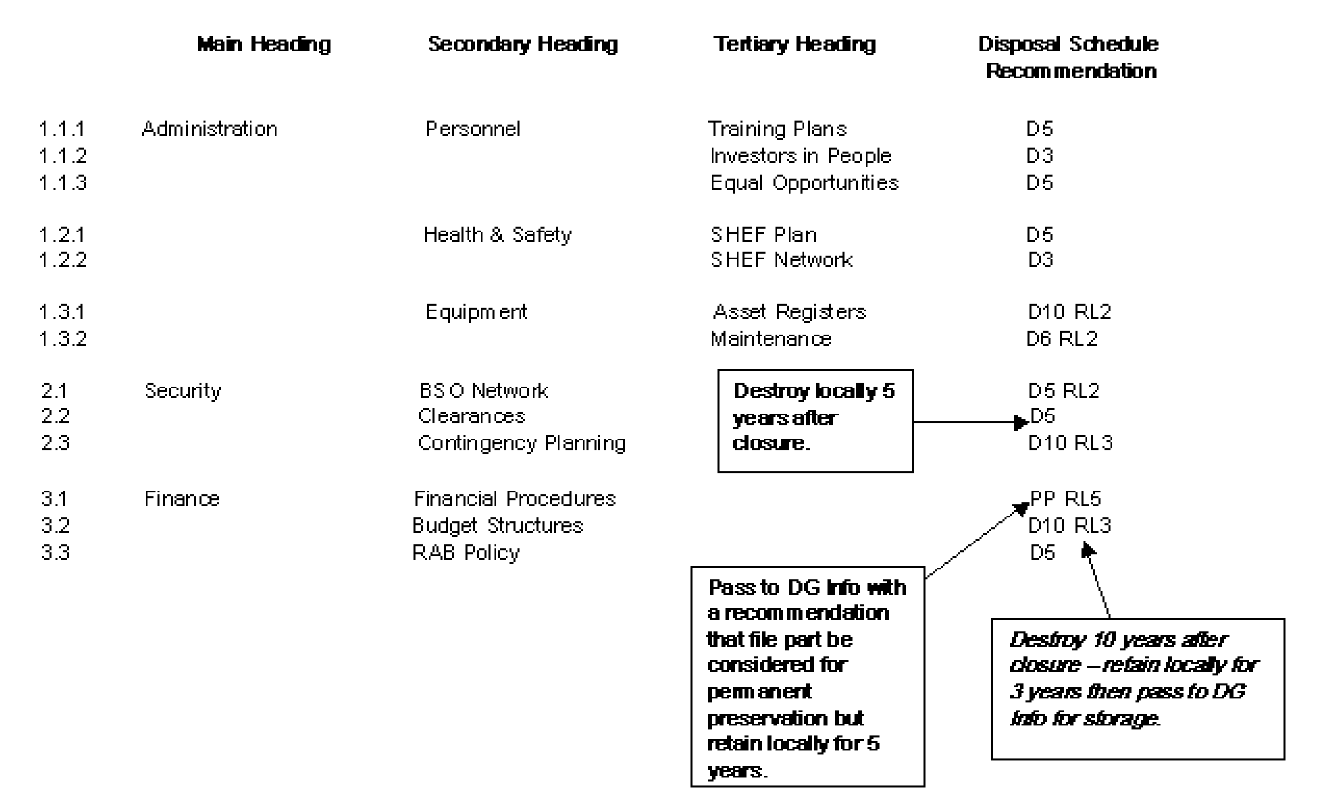
This Page Last Updated: Monday, 20 January 2003 11:57

Queries, Suggestions, etc.

**JSP 441** **Defence Records Management Manual Chapter 5 Annex B**

## EXAMPLE OF A DISPOSAL SCHEDULE

# Disposal Schedule



| | Main Heading | Secondary Heading | Tertiary Heading | Disposal Schedule Recommendation |
|---|---|---|---|---|
| 1.1.1 | Administration | Personnel | Training Plans | D5 |
| 1.1.2 | | | Investors in People | D3 |
| 1.1.3 | | | Equal Opportunities | D5 |
| 1.2.1 | | Health & Safety | SHEF Plan | D5 |
| 1.2.2 | | | SHEF Network | D3 |
| 1.3.1 | | Equipment | Asset Registers | D10 RL2 |
| 1.3.2 | | | Maintenance | D6 RL2 |
| 2.1 | Security | BSO Network | | D5 RL2 |
| 2.2 | | Clearances | | D5 |
| 2.3 | | Contingency Planning | | D10 RL3 |
| 3.1 | Finance | Financial Procedures | | PP RL5 |
| 3.2 | | Budget Structures | | D10 RL3 |
| 3.3 | | RAB Policy | | D5 |

**Destroy locally 5 years after closure.**

**Pass to DG Info with a recommendation that file part be considered for permanent preservation but retain locally for 5 years.**

***Destroy 10 years after closure – retain locally for 3 years then pass to DG Info for storage.***

**Figure 5B1 - Example of a completed Disposal Schedule**

**(i)** The above is an example of an extract of a completed Disposal Schedule. In this example, the records are contained in registered files. The schedule should also include any unregistered records

**(ii)** Note that the schedule identifies each Main Heading and then each subordinate heading by number and title. Each individual file is then listed under the appropriate headings. In this example most files have a three part title (main heading and secondary heading).

**(iii)** Variations on three abbreviations can be used to record all relevant disposal recommendations:

**D** = retain locally and destroy * years after closure (Note that the D prefix **must** be accompanied by the relevant timescale as in the example **2/2** above where "**D5**" denotes "destroy 5 years after date of last enclosure")

**PP** = pass to DG Info-Records with a recommendation that the file merits consideration for permanent preservation. File **3/1** is an example of a file that has been identified as meriting such action.

**RL** = retain locally for a period of time before passage to DG Info-Records for storage or review. (e.g. file **1/3/1** has been annotated "**D10 RL3**" to denote "to be destroyed 10 years after date of last enclosure but retained locally only for 2 years, after which the file will be forwarded to DG Info-Records for storage.")

**(iv)** Each business unit should give consideration as to whether to introduce a blanket policy whereby files which are not marked for early destruction should be passed to DG Info-Records for storage after a specified period (perhaps 2 years after date of last enclosure). Such a policy reflects the fact that most files will not be needed on a regular basis after this period of time and should not be occupying valuable and limited local storage space. Where necessary such files can be called back for reference.

**(v)** Where it is not possible to make a recommendation about the disposal of a file the abbreviation **NR** (no recommendation) is to be used. The records officer/desk officer will need to consider such a file on its merits at the time of file review. Such a course of action should be unusual.

Home Back to Contents Back to Chapter 5 Top of Page Index

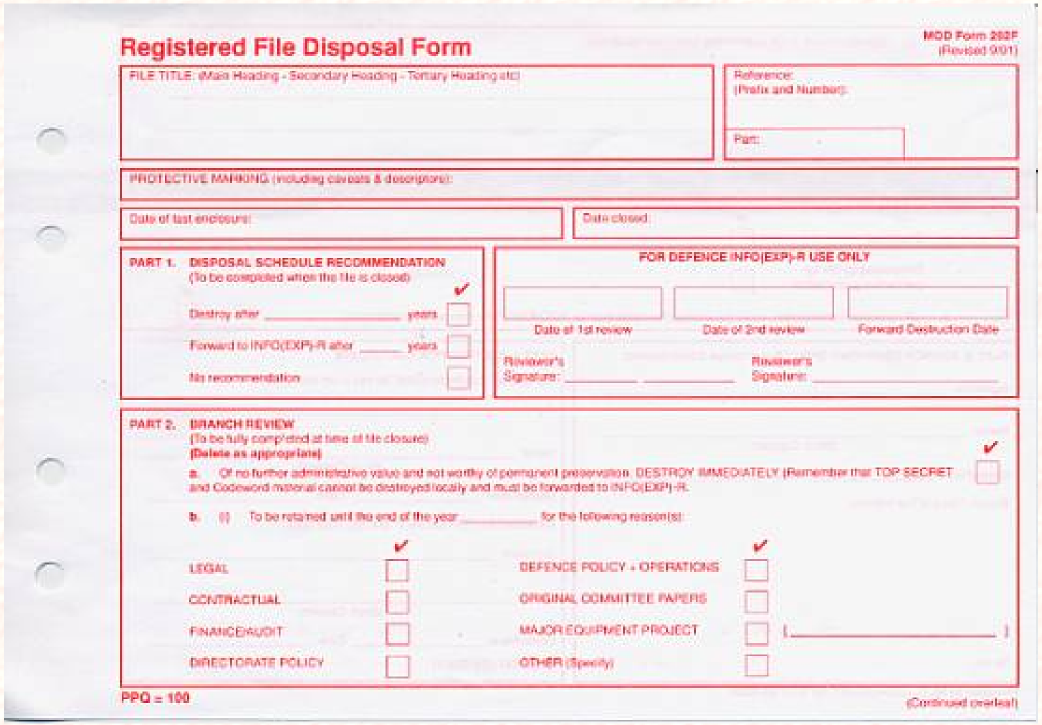
Last updated 20/01/03

This Page Last Updated:
Monday, 27 January 2003 14:58

Queries, Suggestions, etc.

**JSP 441** Defence Records Management Manual
Chapter 5 Annex C

# Example of a Registered File Disposal Form (MOD Form 262F)



MOD Form 262F
(Revised 9/01)

## Registered File Disposal Form

FILE TITLE: (Main Heading - Secondary Heading - Tertiary Heading etc)

Reference:
(Prefix and Number):

Part:

PROTECTIVE MARKING (including caveats & descriptors):

Date of last enclosure:

Date closed:

**PART 1. DISPOSAL SCHEDULE RECOMMENDATION**
(To be completed when the file is closed)

✓

Destroy after ____________ years □

Forward to INFO(EXP)-R after ______ years □

No recommendation □

**FOR DEFENCE INFO(EXP)-R USE ONLY**

Date of 1st review

Date of 2nd review

Forward Destruction Date

Reviewer's Signature: ____________ ____________

Reviewer's Signature: ____________

**PART 2. BRANCH REVIEW**
(To be fully completed at time of file closure)
**(Delete as appropriate)**

✓

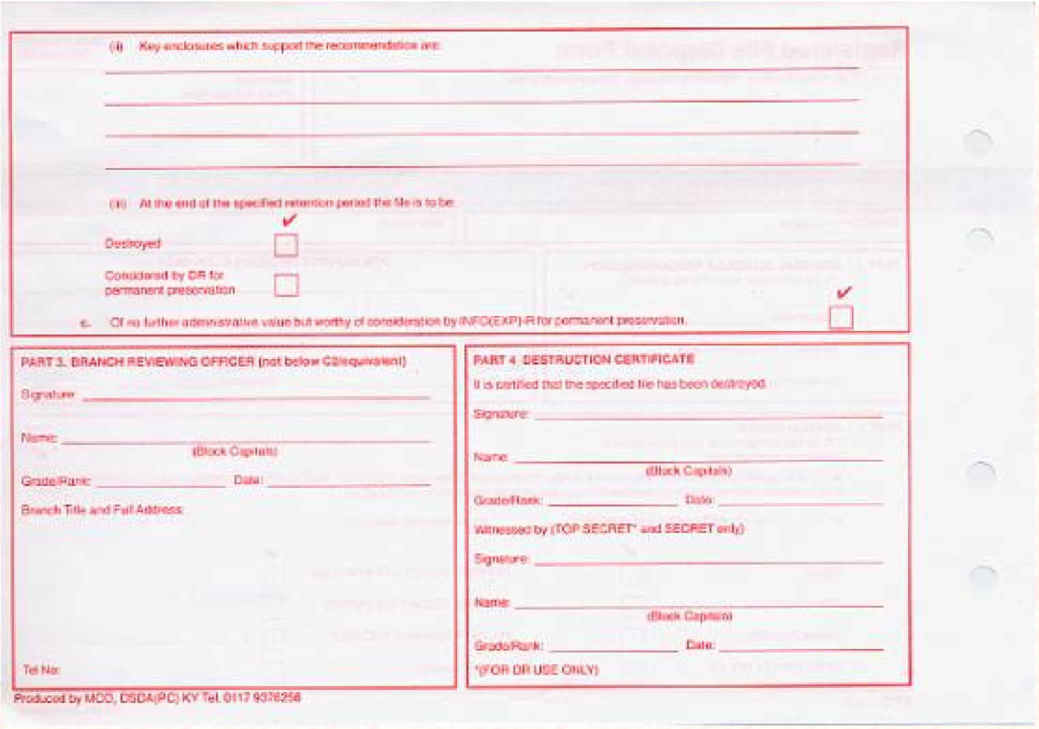
a. Of no further administrative value and not worthy of permanent preservation. DESTROY IMMEDIATELY (Remember that TOP SECRET and Codeword material cannot be destroyed locally and must be forwarded to INFO(EXP)-R. □

b. (i) To be retained until the end of the year ________ for the following reason(s):

| | ✓ | | ✓ | |
|---|---|---|---|---|
| LEGAL | □ | DEFENCE POLICY + OPERATIONS | □ | |
| CONTRACTUAL | □ | ORIGINAL COMMITTEE PAPERS | □ | |
| FINANCE/AUDIT | □ | MAJOR EQUIPMENT PROJECT | □ | (____________) |
| DIRECTORATE POLICY | □ | OTHER (Specify) | □ | |

PPQ = 100

(Continued overleaf)



(i) Key enclosures which support the recommendation are:

______________________________

______________________________

______________________________

______________________________

(ii) At the end of the specified retention period the file is to be:

✓

Destroyed ☐

Considered by DR for permanent preservation ☐

✓

c. Of no further administrative value but worthy of consideration by INFO(EXP)-R for permanent preservation. ☐

PART 3. BRANCH REVIEWING OFFICER (not below C2/equivalent)

Signature: ______________________________

Name: ______________________________
(Block Capitals)

Grade/Rank: ______________ Date: ______________

Branch Title and Full Address:

Tel No:

PART 4. DESTRUCTION CERTIFICATE

It is certified that the specified file has been destroyed.

Signature: ______________________________

Name: ______________________________
(Block Capitals)

Grade/Rank: ______________ Date: ______________

Witnessed by (TOP SECRET* and SECRET only)

Signature: ______________________________

Name: ______________________________
(Block Capitals)

Grade/Rank: ______________ Date: ______________

*(FOR DR USE ONLY)

Produced by MOD, DSDA(PC) KY Tel. 0117 9376256

**Figure 5C.1 - Registered File Disposal Form (Front and Back)**

(i) Chapter 4 (para 4.17) outlines the factors which determine when a registered file should be closed and the action to be taken at that time.

(ii) When a file is closed a Registered File Disposal Form (MOD Form 262F) is to be raised and placed in the file in accordance with the instructions in Chapter 4, para 4.18. At that time the Disposal Schedule is to be consulted to determine what recommendation has been made about the appropriate retention period and method of disposal. The disposal schedule recommendation should be noted in section I of the 262F and the file should then be passed to the desk officer responsible for reviewing it and completing the remainder of the form.

(iii) The desk officer responsible for carrying out the review must then consider the recommendation at section I of the 262F and either endorse or amend it. Before doing so the file minute sheet should be checked to see whether details of any significant enclosures have been recorded (see Chapter 4, para 4.9.1).

(iv) The 262F should then be completed and signed by an officer of at leastC2 (or equivalent) grade (where necessary the desk officer must arrange for the form to be signed by the records officer or a line manager). If the ultimate recommendation is that the file should be retained for an extended period for administrative purposes, or that the file warrants permanent preservation, the specific enclosures which justify that recommendation (which should be identified on the file minute sheet) should be recorded on the 262F. If there are a large number of enclosures which justify such a recommendation only the key enclosures need be identified.

**Failure to complete the form thoroughly may result in the file being returned to the business unit with a request that more detailed information be provided, or may lead to the file's early destruction.**

Home Back to Contents Back to Chapter 5 Top of Page Index

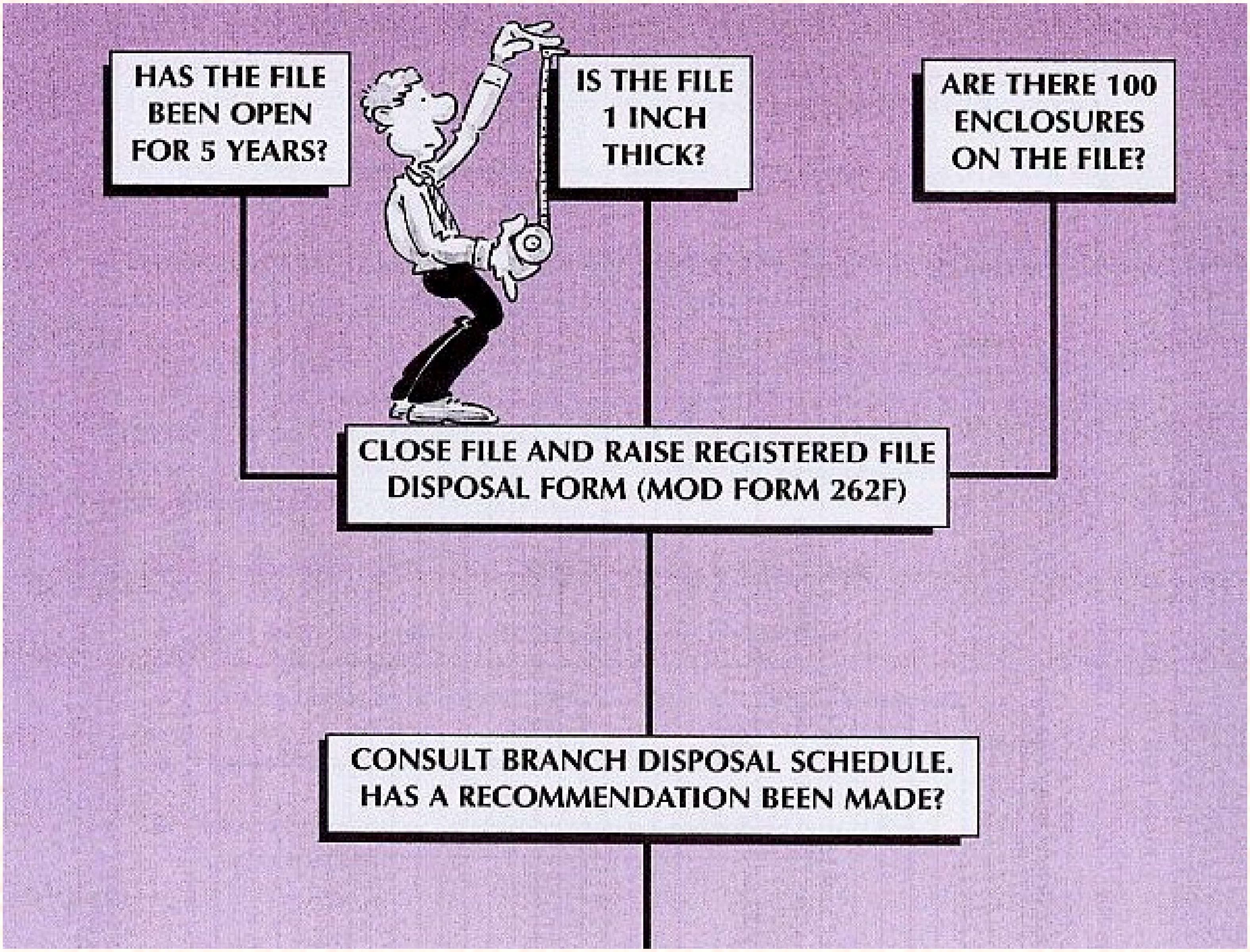
This Page Last Updated: Monday, 11 March 2002 12:09

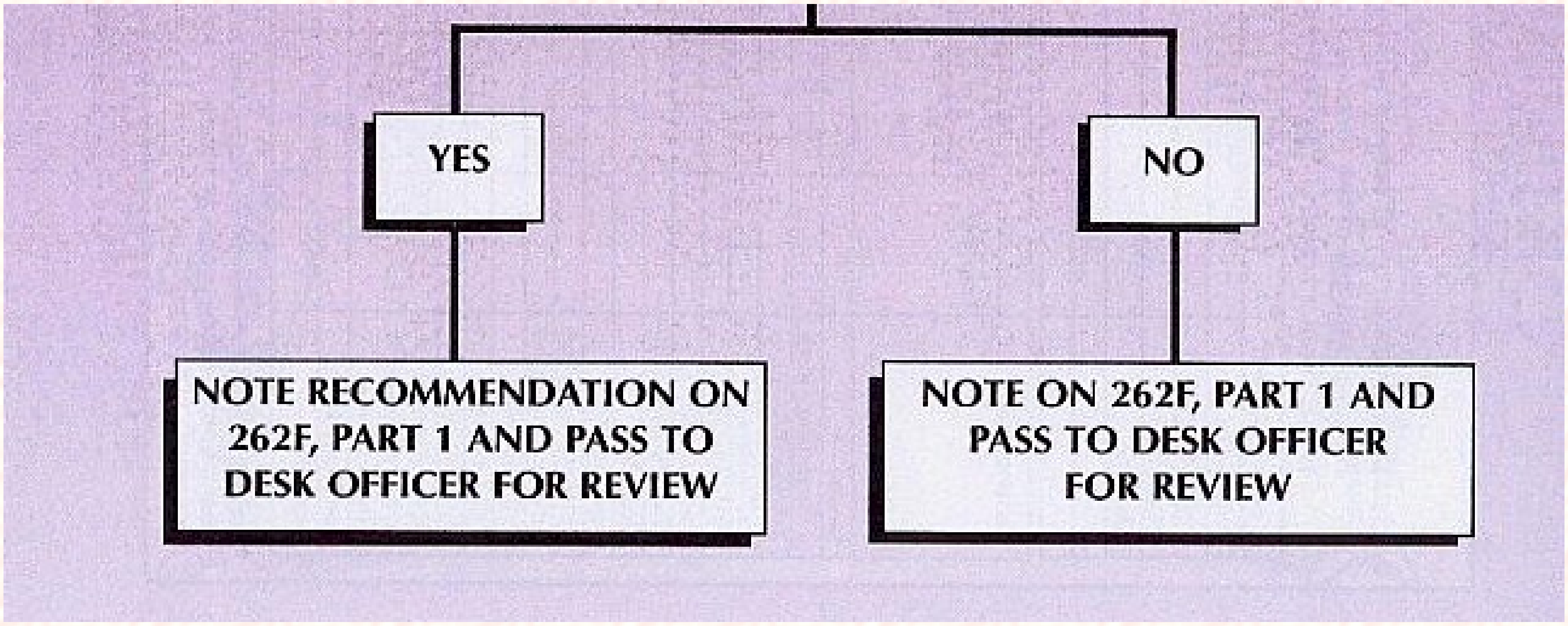
Queries, Suggestions, etc.

**JSP 441** Defence Records Management Manual Chapter 5 Annex D

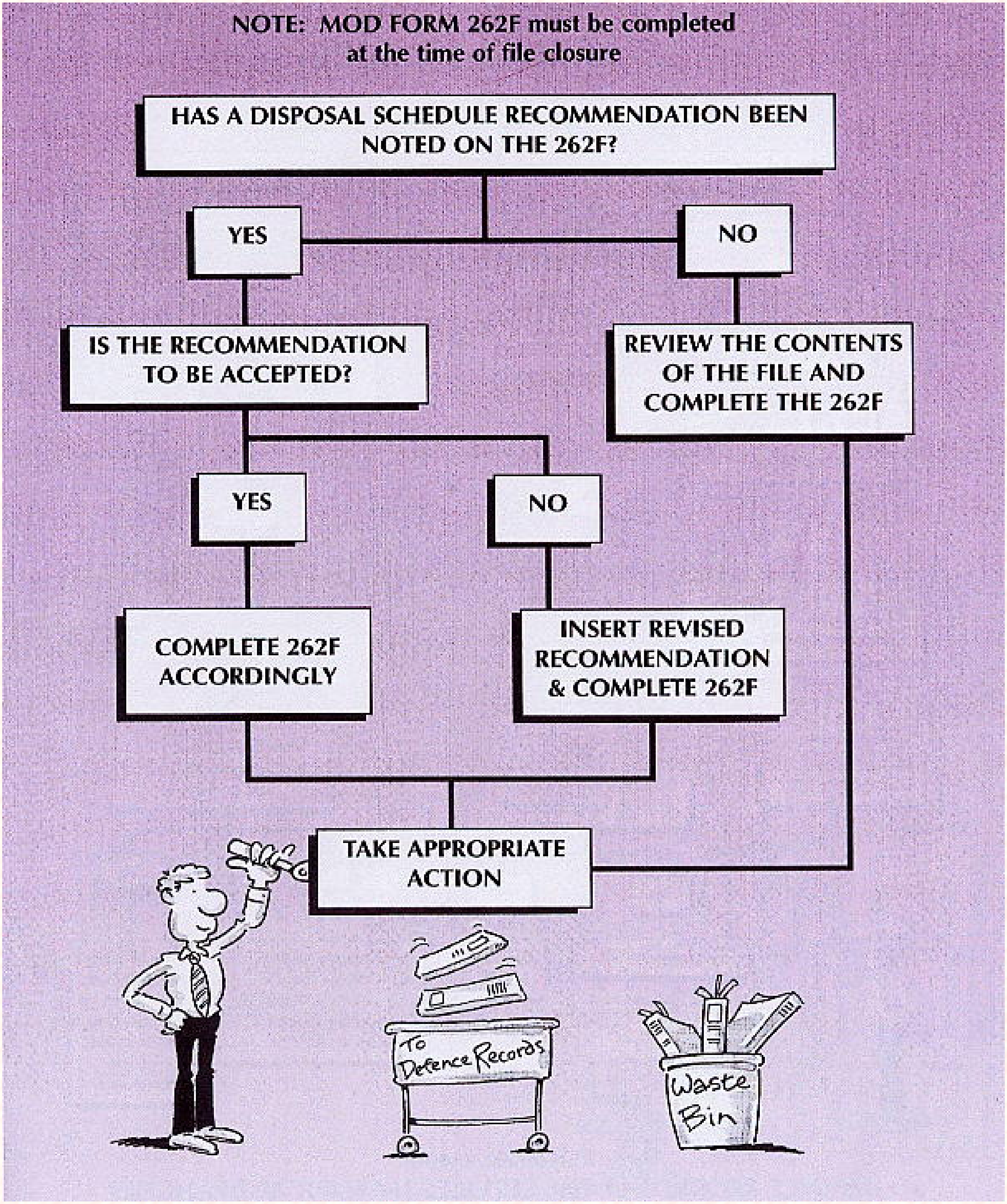
## File Review - Aide Memoir

# File Review - Aide Memoir


HAS THE FILE BEEN OPEN FOR 5 YEARS?
IS THE FILE 1 INCH THICK?
ARE THERE 100 ENCLOSURES ON THE FILE?
CLOSE FILE AND RAISE REGISTERED FILE DISPOSAL FORM (MOD FORM 262F)
CONSULT BRANCH DISPOSAL SCHEDULE. HAS A RECOMMENDATION BEEN MADE?


YES
NO
NOTE RECOMMENDATION ON 262F, PART 1 AND PASS TO DESK OFFICER FOR REVIEW
NOTE ON 262F, PART 1 AND PASS TO DESK OFFICER FOR REVIEW

# Completing the Registered File Disposal Form: MOD Form 262F



NOTE: MOD FORM 262F must be completed at the time of file closure

HAS A DISPOSAL SCHEDULE RECOMMENDATION BEEN NOTED ON THE 262F?

YES

NO

IS THE RECOMMENDATION TO BE ACCEPTED?

REVIEW THE CONTENTS OF THE FILE AND COMPLETE THE 262F

YES

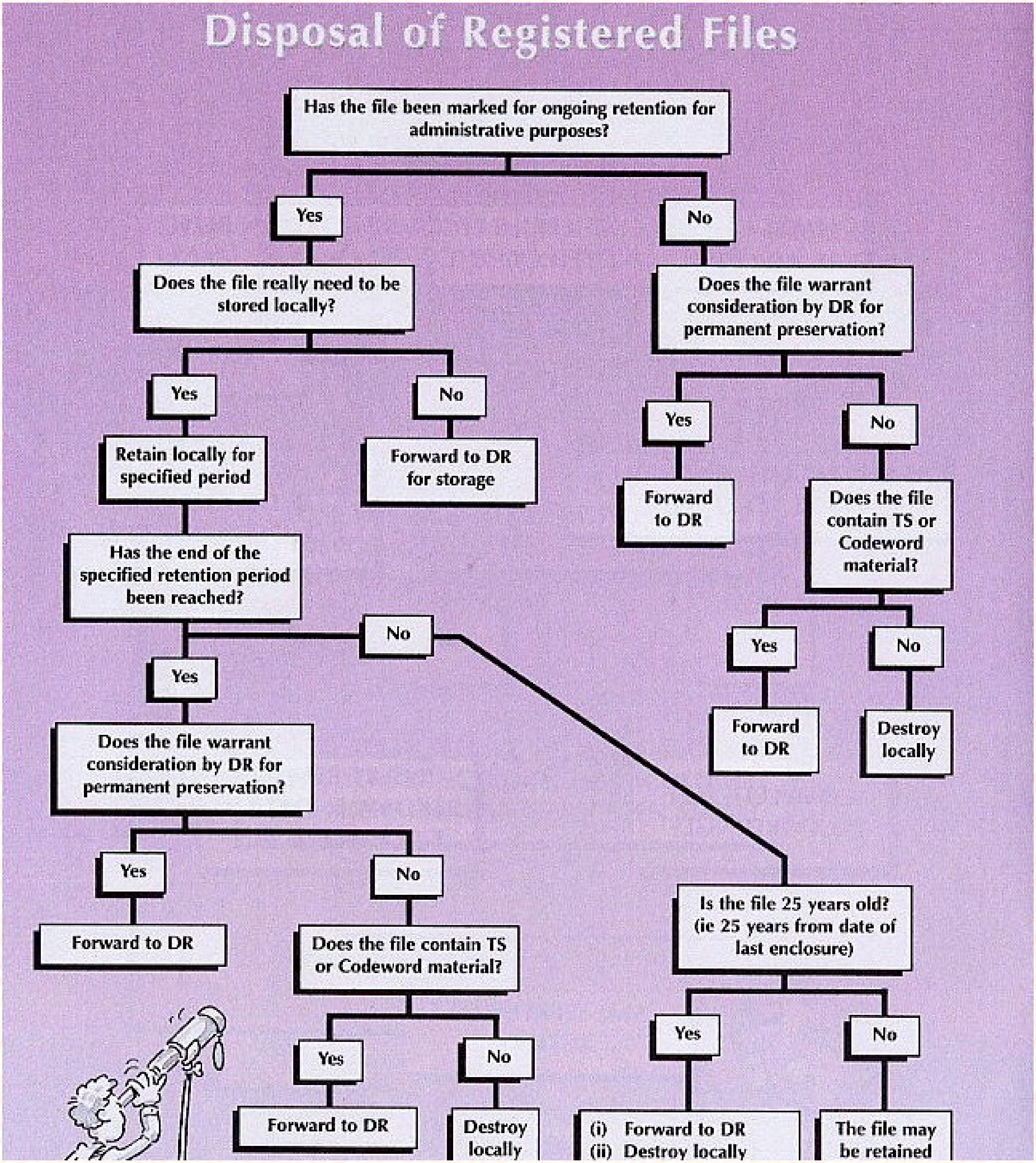
NO

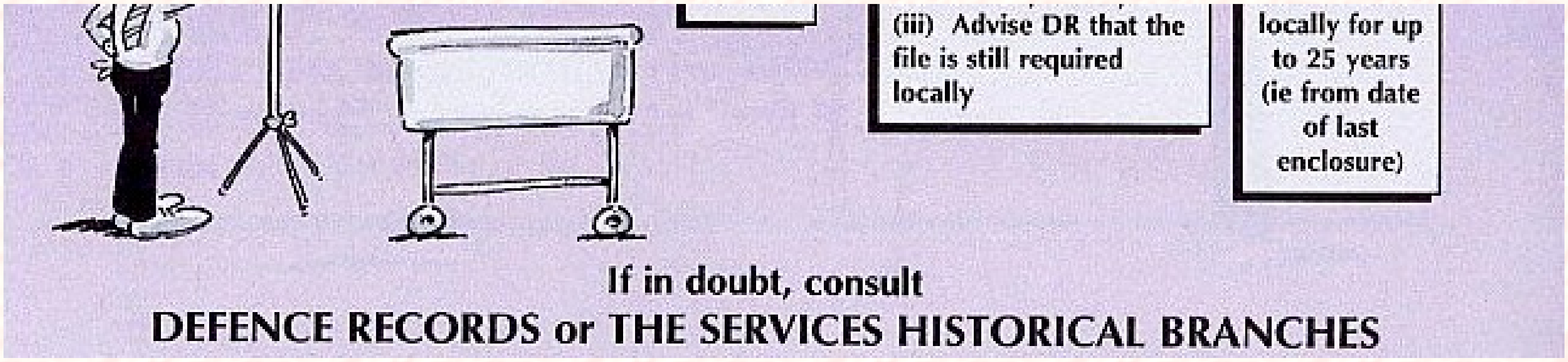
COMPLETE 262F ACCORDINGLY

INSERT REVISED RECOMMENDATION & COMPLETE 262F

TAKE APPROPRIATE ACTION

# Disposal of Registered Files


Disposal of Registered Files
Has the file been marked for ongoing retention for administrative purposes?
Yes
No
Does the file really need to be stored locally?
Does the file warrant consideration by DR for permanent preservation?
Yes
No
Yes
No
Retain locally for specified period
Forward to DR for storage
Forward to DR
Does the file contain TS or Codeword material?
Has the end of the specified retention period been reached?
No
Yes
No
Yes
Forward to DR
Destroy locally
Does the file warrant consideration by DR for permanent preservation?
Yes
No
Forward to DR
Does the file contain TS or Codeword material?
Is the file 25 years old? (ie 25 years from date of last enclosure)
Yes
No
Yes
No
Forward to DR
Destroy locally
(i) Forward to DR
(ii) Destroy locally
The file may be retained

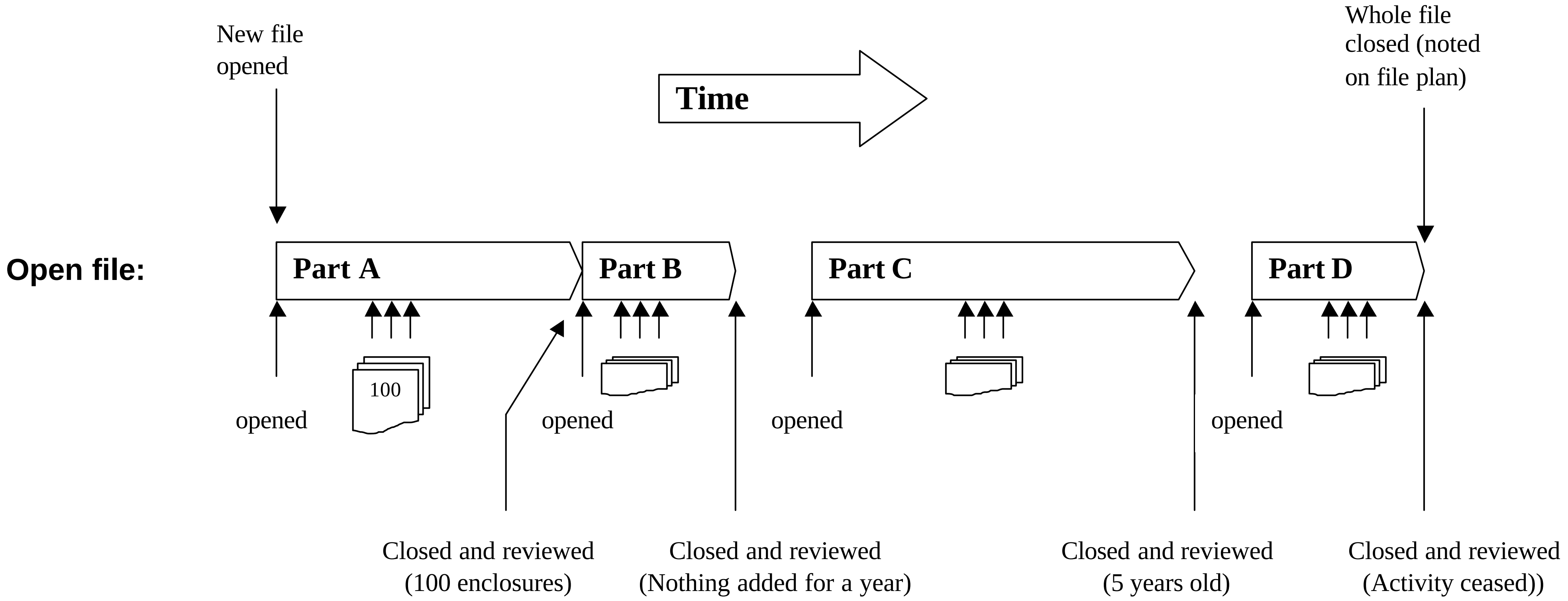

(iii) Advise DR that the file is still required locally
locally for up to 25 years (ie from date of last enclosure)
If in doubt, consult
DEFENCE RECORDS or THE SERVICES HISTORICAL BRANCHES

Home Back to Contents Back to Chapter 5 Top of Page Index

Last updated 11/03/02

# Defence Records Management Manual
# Chapter 5 Annex E

## THE LIFE-CYCLE OF AN OPEN FILE

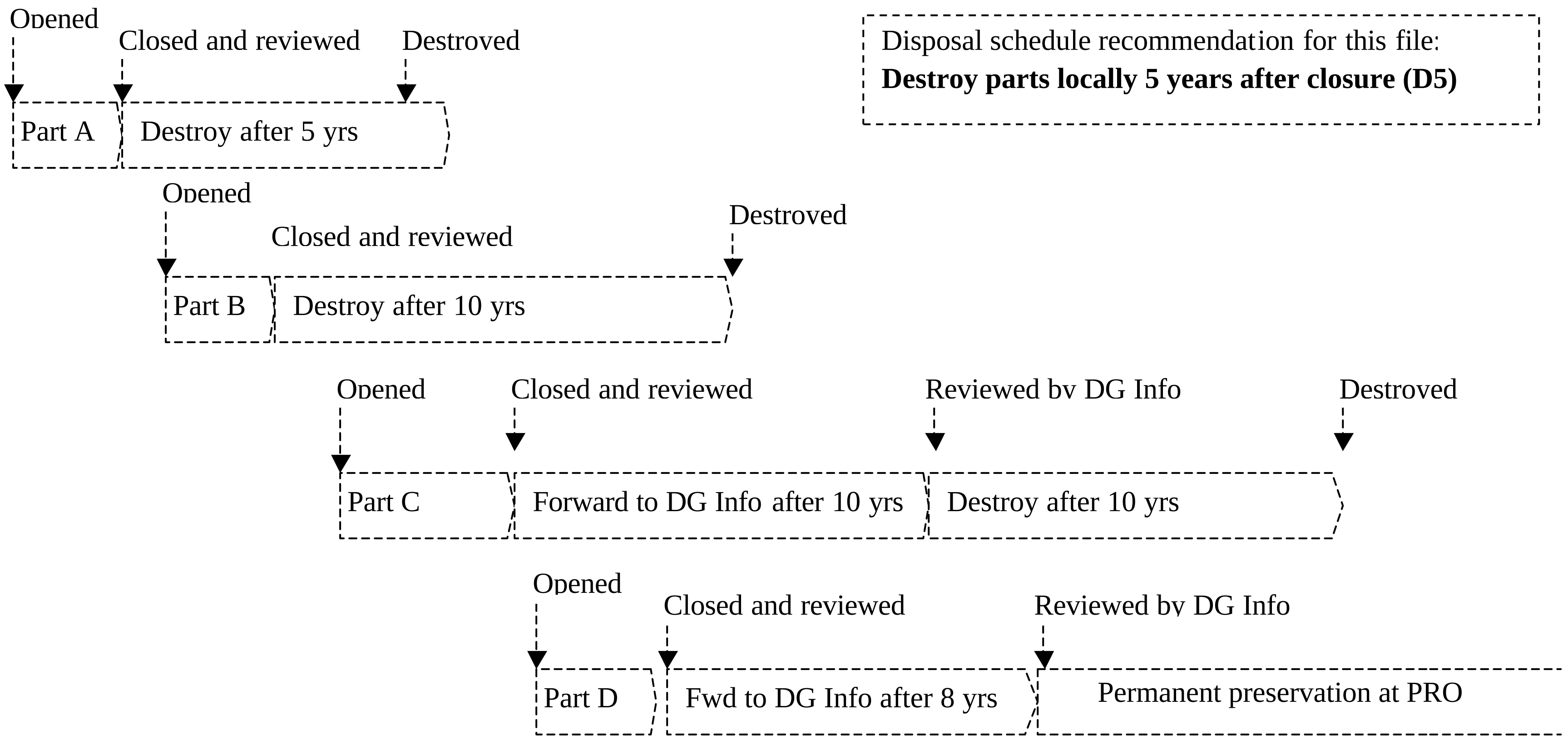

New file opened
Time
Whole file closed (noted on file plan)
Open file:
Part A
Part B
Part C
Part D
opened
100
opened
opened
opened
Closed and reviewed (100 enclosures)
Closed and reviewed (Nothing added for a year)
Closed and reviewed (5 years old)
Closed and reviewed (Activity ceased))

**Notes:**

- Here is the life-cycle of a typical open file which over time needs to be split into four parts A,B,C and D.
- Each new part is only opened when there is an enclosure to file on it. Note that this can result in time gaps between the parts.
- Parts are closed for several reasons: 100 enclosures (Part A), nothing added for one year (Part B), the part is 5 years old (Part C).
- Eventually the activity associated with the file totally ceases so there is no longer a need for the file. Its final part (Part D) is closed and the whole file is recorded as closed on the file plan.

# Defence Records Management Manual
# Chapter 5 Annex F

## THE LIFE-CYCLE OF A CLOSED FILE



Disposal schedule recommendation for this file:
**Destroy parts locally 5 years after closure (D5)**

**Notes:**

- Here is the life-cycle of a closed file. It's disposal schedule recommends local destruction 5 years after closure.
- Over time the file's four parts A, B, C, D are disposed of in various ways. **NB. In practice it would be highly unusual for parts of the same file to have such widely differing disposals. This example is for illustration only.**
- Part A follows the disposal schedule recommendation and is destroyed 5yrs after closure
- At Part B the reviewer decides to extend the retention period to 10 years at which point the file part is destroyed.
- At Part C the reviewer decides to transfer the file part to DG Information as it may merit permanent preservation. The DG Information reviewer decides that permanent preservation is not merited and marks the file for destruction after a further 10 years.
- At Part D the reviewer decides to transfer the file part to DG Information as it may merit permanent preservation. The DG Information reviewer agrees that Permanent preservation is merited and arranges transfer to the PRO.

**This Page Last Updated:**
**Tuesday, 11 March 2003 13:56**

Queries, Suggestions, etc.

**JSP 441** | **Defence Records Management Manual Chapter 6**

# Electronic Records Management Systems

# 6.1 Introduction

6.1.1. Most organisations in the MOD are dependent on electronic office automation systems. Although commonly used packages such as Microsoft Office support the creation and communication of electronic documents (word-processor documents, spreadsheets, calendars, diagrams etc) they lack the facilities required to preserve them as properly managed records. Such systems do not meet the standards of authenticity, integrity, reliability, security and accessibility necessary for the longer term needs of the originator, the department in general, the courts, auditors and the Public Record Office. The implementation of Electronic Records Management Systems (ERMS) following the policy and guidance set out below is therefore essential for MOD to manage its records in a thorough and uniform manner and hence achieve the full benefits of exploiting its information to the full.

6.1.2. This chapter sets out MOD advice, guidance and standards for the management of records using an ERMS. Organisations without ERMS should follow the standards laid out in JSP713 - Managing Electronic Documents in a Shared document Store – which is one of the JSP700 series of guides on Electronic Working Practice. JSP713 describes how to manage documents produced by standard office automation packages such as MS Office. Any documents which then need to be retained for long term use must be kept as paper records following the guidance set out in the other chapters of this manual.

6.1.3. The term ERMS refers to that subset of functions concerned with the electronic management of records. ERMS can be implemented as freestanding applications that interface with standard office automation packages, but it is becoming increasingly common for ERMS to be implemented as part of larger integrated Information Management packages often referred to as an Electronic Document and Record Management System(s) (EDRMS). MOD is developing an Electronic Document and Record Management (EDRM) capability therefore to avoid confusion about whether the solution will be provided as a freestanding application or an integrated capability, the remainder of this chapter will refer to EDRM capability as EDRMS.

6.1.4. It is an aim for the whole of MOD to share a common EDRMS, however initial implementations of EDRM will operate in isolation until a common capability on the Defence Information Infrastructure (DII) is implemented. It is therefore important to ensure a high degree of uniformity by adherence to a single policy thus achieving commonality and helping to ensure that good quality records are produced, managed and shared across MOD.

6.1.5. Records take many different forms and it is important to recognise that the Public Records Acts, Data Protection Acts, Freedom of Information Act, Environmental Information Regulations 2002 and all other acts of Parliament which refer to the keeping of public records apply equally to all records whether hard copy or electronic.

6.1.6. MOD’s Corporate Policy for Electronic Records (CPER) is at Annex A. The CPER defines the principles governing the production and management of electronic records. Much of what it says applies equally to records in other forms. The aim of the CPER and the more detailed policy and guidance in this chapter is to enable MOD to fully exploit the information contained in its records while also meeting its legislative obligations.

# 6.2 Background

6.2.1. *Documents* are defined as any tangible information received or produced by the department. *Records* are those *documents* that support some official activity or decision and need to be preserved for future reference. Legally, <u>any</u> document produced by or held by MOD is a *public record* and it is important to recognise this when considering whether appropriate records management procedures are in place. *Document management* systems support the creation and communication of *documents* used in support of business functions. They can be freestanding or integrated with functions such as scanned image management, workflow management and web publishing. *Record management* is the capture, preservation, retrieval, review and destruction of *records*. This chapter is concerned with electronic *record management*.

6.2.2. Electronic record management is concerned with the preservation, for as long as necessary (and no longer), of the documents generated by, or used by, a business unit. These documents should provide evidence of the activities that took place, establish exactly what happened and enable others to understand why decisions were taken.

6.2.3. Once a document has been chosen for preservation – short or long term - it becomes a part of the department's record and then by definition, it is immutable, i.e. it must not be amended. Most records lose their importance over time and many are no more than ephemeral. However, they may be vital to the business unit that created them or essential to the department as a whole and some may be of interest to the nation and individual members of the public. A small minority of records will ultimately be worthy of permanent preservation in the National Archive at the Public Record Office.

6.2.4. Good record management has always been important but will become increasingly so with the advent of the Information Age. Under Freedom of Information (FOI) and Environmental Information Regulations (2002) (EIR) legislation the department is obliged to provide prompt, accurate replies to questions raised by members of the public and non-government organisations. Records will need to be maintained to high standards to meet the needs of the department as a whole. Hence they must be treated as corporate resources.

6.2.5. Records must also be seen to be trustworthy. In our increasingly litigious society they may be required to substantiate or refute legal claims and it may be necessary to demonstrate their authenticity and integrity in a court of law. Good EDRM practice will ensure that through time records:

- Are present.
- Can be accessed by those entitled.
- Can be understood.
- Can be trusted.
- Can be deleted when no longer required.

6.2.6. It is important that the principles of good record management expounded in the rest of JSP441 are well understood. To be of full use, records need to be valued. EDRM can help relieve the burden of record keeping but only if applied conscientiously and intelligently.

6.2.7. To provide further background and clarification, the following diagram describes the record management hierarchy used within this chapter and the aggregation levels referred to in the Metadata Elements table at Annex B.

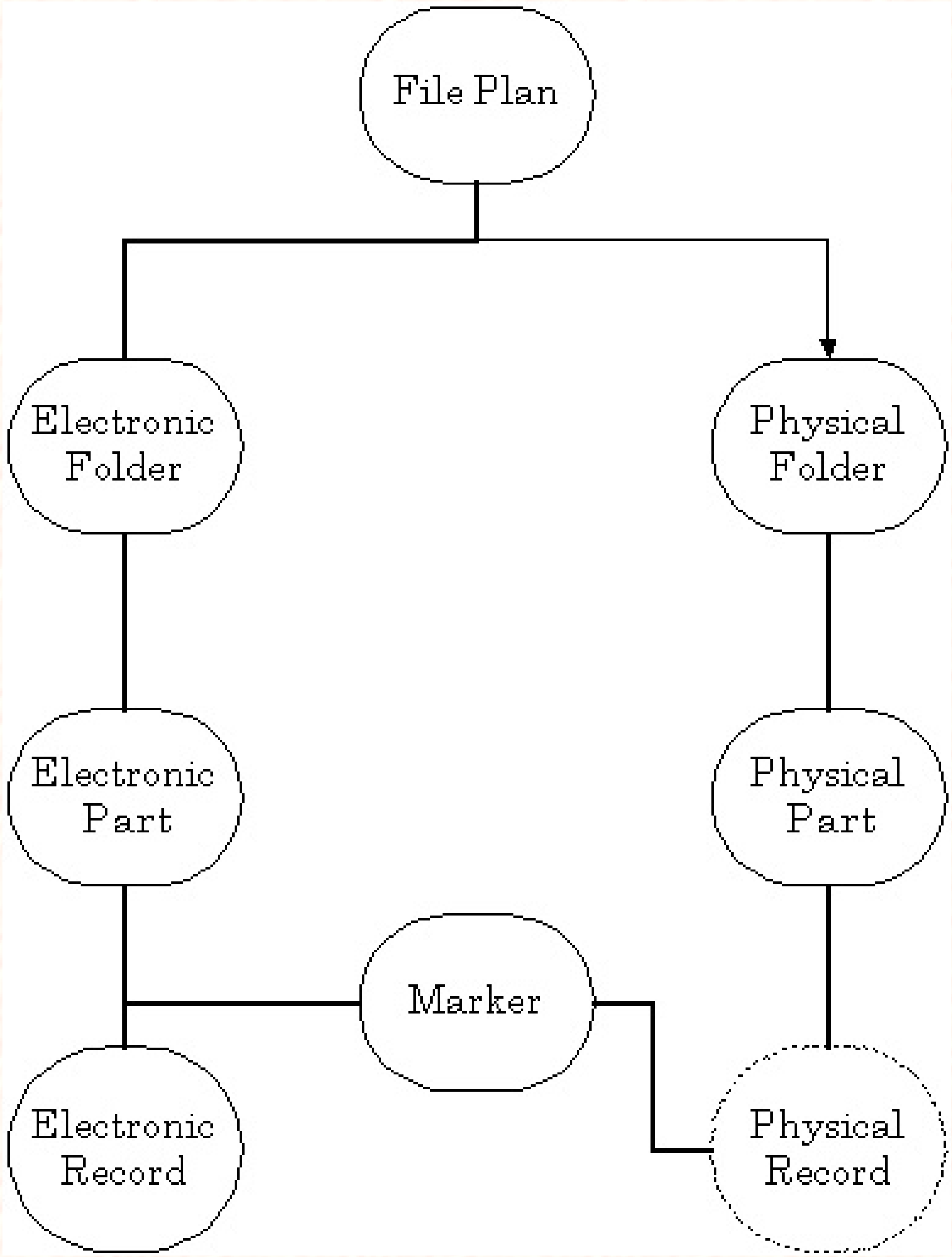


**Diagram 1 - Record Management Hierarchy**

6.2.8. *Fileplan*. A fileplan is a representation of the business of the business unit, within a structure that is best suited to support the conduct of that business and meet records management needs. A fileplan does not itself contain records; it is an attribute against which a folder is categorized (or classified).

6.2.9. *Folder*. An electronic folder is a (virtual) container for records (segmented by parts where necessary) and is attributed to the fileplan. A folder is the primary unit of record management and is constituted of metadata (see section 6.9 below ). Some of this metadata is inherited from the fileplan to which the folder belongs; and some may be inherited by the records that the folder itself contains. There may be many folders within a fileplan.

6.2.10. *Physical Folder*. A physical folder is an entry within the fileplan for a legacy physical or paper folder, which is not itself held within the system, but is physically located elsewhere. Such an entry provides information about the folder and its location. There are two ways in which a physical folder is represented:

- Where the physical folder stands on it own, and has no relationship with an electronic folder, other than being allocated an appropriate file reference number in the fileplan hierarchy.

· Where the physical folder represents the physical element of an electronic folder and has the same title. The physical and electronic folder together, constitute a hybrid folder (see section 6.3.7 below ). Hybrid folders must be managed as one for purposes of retrieval and disposal.

6.2.11. *Part*. The management of records is performed primarily at the folder level rather than on an individual record basis. A part is a segment of a folder (either physical or electronic). The folder is segmented to allow a whole group of records to be managed together and the same actions taken on all records in that group at the same time. Where more than one part exists, the end user will normally work with the most recent part. A folder will contain at least one – the initial – part, and may contain many parts.

6.2.12. *Electronic Record.* An electronic record is constituted of both content and metadata; it may be a single object, such as a Word document, or a set of closely bound objects that are meaningfully treated as one, such as a web page or multimedia document. A folder and part(s) may contain many records.

6.2.13. *Marker (for a Physical Record).* A marker is an entry for a physical record that is made in an electronic folder. The physical record itself is held outside of the system and the marker is the metadata for that record. Typically, a marker might be used to describe items such as large building plans, videotapes, or a database, which can neither be contained in a conventional physical file nor easily be digitized.

# 6.3 Requirements of EDRM

6.3.1. The following paragraphs give a summary of the major features of EDRM, however a user requirements document, more information about which can be found on the DG Info Website, provides more in-depth information on the typical facilities expected of an EDRMS.

6.3.2. *Organisation*. Decisions about retention, disposal and destruction of documents need to be considered at the subject (or folder) level not at the document level. In a conventional paper filing system this corresponds to a file, which is usually split over time into a series of file parts. An EDRMS similarly needs to be able to hold records according to a fileplan (see section 6.7 below ) and to subdivide them into manageable units of information e.g. no more than 100 separate objects in each.

6.3.3. *Declaration*. If a document is to be maintained within an EDRMS, then, in addition to the capture of the content itself (see section 6.8 below ), the system will need to capture its attributes e.g. title, file reference, date of creation, originator, keywords (attributes like this are often referred to as *metadata* (see section 6.9 below )) and its history. It is essential that the contents of records once captured cannot be amended. Comprehensive metadata is essential for accessing and managing records successfully. Some or all of the metadata will also survive for a period of time after the contents have been destroyed e.g. a record’s history, in the form of an audit trail, records creation, access, review, and eventual disposal (see section 6.9.9). The system should be capable of capturing documents in a wide range of electronic forms (e.g. word-processor documents, spreadsheets, e-mail, web-pages, presentations, desktop publishing documents, scanned images, multi-media documents incorporating digitised sound and video).

6.3.4. *Retention and Disposal*. All records need an associated policy on retention and disposal that has previously been set at the folder level (see section 6.12 below ). The EDRMS must have a facility to record that policy and automatically bring record collections to the attention of the BRO when a decision on retention, transfer or destruction is needed. The EDRMS should also be capable of deleting just the record content leaving behind the metadata and audit trail.

6.3.5. *Access Management*. Records containing sensitive information need to be protected from system users who do not have the corresponding access rights (see section 6.16 below ). An EDRMS should recognise several types of user according to their function including, for example:

· Staff who can declare new documents as records.

· Registry staff / Information managers who can register non-electronic documents and manage their retention, review and eventual disposal.

· The Branch Records Officer (BRO) who manages the overall filing scheme and approves new file references (see Chapter 3 for BRO TORs).

· Staff permitted to update records / metadata, e.g. to amend the protective marking of a record.

· Staff in other business units permitted to view the record.

· DG Info staff accepting records into the Defence Archive or authorising disposition action on the record.

6.3.6. *Audit and Authentication*. An EDRMS must ensure the availability and authenticity (see section 6.20 below ) of the records it holds over long periods for some types of information. Secure and resilient systems are required. If any of the records stored need to be produced as legal evidence then the integrity of the system may be challenged in court and will need to demonstrate strict adherence to departmental and system policy (see section 6.19 below ). Regular audits may be required to confirm that integrity is being maintained and the system should provide facilities to support such audits (see section 6.20 below ).

6.3.7. *Hybrid Systems.* Whilst the majority of new records will be electronic, some records, both existing and newly created, are for practical reasons likely to be retained on various media such as microfilm, videotape as well as paper. An EDRMS must offer the capability of managing non-electronic records and their metadata as well as electronic records. A folder containing records in mixed electronic and physical formats is referred to as a *hybrid folder* (see also section 6.10 below ).

6.3.8. *Indexing and Retrieval*. EDRMS offer the advantage, over paper systems, of being able to access data using a range of search criteria and complex queries (see section 6.11 below ). Electronic records may be searched at a number of levels such as: using existing key fields like the file reference; by searching the metadata (such as document title, originator, data of issue) or by searching the record content. Complex searches may employ a combination of methods.

6.3.9. *Import and Export*. To support the long term preservation of records - during which time the original EDRMS may be upgraded and the original business unit re-organised - the system must be able to import and export blocks of records, with their associated metadata and audit trails, to and from various media and cater for a complete download and upload to a new system (see section 6.13 below ). There should also be tools available to facilitate transfer between disparate systems.

6.3.10. *Non-functional Aspects.* Good record management must be made as easy as possible, particularly at the record capture stage. Ideally it should be easier to file properly than not to file at all, with as few keystrokes as possible required to effect each transaction (see section 6.22 below ). The EDRMS should be fully integrated with any office automation package in use so that it appears to be a natural extension of the package. For example, it should be possible to file directly into the EDRMS from within the word-processor, spreadsheet or mail facilities without the need for a separate file transfer. The performance of the overall package should not slow users down. Good industry standards in other respects such as scalability, maintainability, support, help facilities and documentation also need to be considered.

# 6.4 Record Types and Periods of Retention

6.4.1. In order to understand the requirements for managing a set of records, it is first necessary to understand the nature of the information held in those records. Record management requirements can vary enormously and no two business units are likely to be the same in this respect.

6.4.2. The different types of information held within any particular business unit might include:

· Administrative Records – These records are produced in large volumes. Generally they have low retention values and are usually disposed of within 1 to 7 years after the date of creation.

· Case Records – The retention periods for these records are usually defined by an individual's age and life span unless a statutory or a long-term operational requirement defines a period for their continued retention. For example, records relating to criminal cases may be retained for 75 years or more.

· Command, Control and Operational Records – Some records in these categories can have a long life span and should, in many cases, be considered for permanent preservation.

· Estates and Accommodation Records – These records include a substantial amount of administrative records with a low retention value, however certain records may be retained for much longer periods. For example:

· Legal records – estate title, leasehold documentation, etc., should be retained for at least the occupancy period.

· Policy records – surveys, policy studies etc., retention varies between 10 to 25 years but there may be records relating to important aspects such as disposal of potentially hazardous substances on sites or other health and safety issues that should be kept for much longer periods of time.

· Finance Records – These records normally have a short working life of about two years. Generally there is no legal requirement to retain these records beyond seven years.

· Health and Safety Records – As well as some statutory requirements that need to be complied with, there are those records that can have a very long retention requirement. Especially in cases involving exposure to radiation or contamination where the safety implications as a result of the contamination may only arise decades after the initial event. A retention period of up to 100 years may be required in some cases.

· Personnel Records – The retention periods for these records may vary but some should be kept for very long periods. Examples include:

· Documents that have a bearing on pension entitlement should be kept for up to 100 years from date of birth.

· Military Service personnel appraisal reports are to be kept for 100 years.

· Civilian Staff appraisal records are normally kept as separate sub-sets of personal files. If kept in annual sets, they should be destroyed on a rolling basis.

· Medical records are normally filed as a separate sub-set of individual personal files to allow for separate retention. In some instances where they relate to, for example, exposure to radiation, these may be kept for up to 100 years.

· Policy Records – These are normally retained for at least 25 years, and in cases where the records relate to the development of primary legislation, may be marked for permanent preservation.

· Scientific, Technical and Research Records – Records of the more important aspects of scientific, technological or medical research and development are normally retained as a long term research resource for other scientific researchers. Retention periods may differ, as some business units may retain these records as part of their permanent library, whilst others may consider them as case files and dispense with them after 10 years. Reports for these types of records are normally preserved, whilst the supporting information is not, however their administrative value could be long, i.e. Porton Down and paper records covering the volunteer programme go back to the 1950's.

· Transaction Records – These records record specific events that have a finite life, i.e. the award of a contract allocated to a named contractor to commission a particular task. Depending on the nature of the transaction, the retention period may vary between 6 to 25 years.

6.4.3. The varying management requirements for each of the types of information listed above also need to be considered. Factors to be considered include:

· Operational requirements.

· Business requirements.

· MOD corporate requirements.

· Public access requirements.

· Legal and statutory requirements.

· Human life expectancy.

· Volume of records likely to be generated.

· Sensitivity.

· Accessibility.

6.4.4. For all record types, including those mentioned above, it is necessary to consider what documents will become records. Some documents may be regarded as purely ephemeral and will not need to be filed as records at all. Documents that provide evidence that a particular action was taken, support decisions made, or are deemed to have some potential worth in the future, are obvious candidates for records.

6.4.5. Declaring a document to be a record is a formal point of transition at which it passes into corporate ownership, i.e. once designated as a record, the document is no longer managed by the creator but by the business unit as part of its corporate information resources. The record should not thereafter be capable of change, and should be placed within a disposal / retention schedule where it will be retained for a set period. When the retention period expires it can be destroyed, or if merited, transferred to the Public Record Office for permanent preservation.

# 6.5 The Transition to Electronic Records

6.5.1. MOD is committed to both the Modernising Government target that by 2004 all newly created records will be electronically stored and retrieved, as well as achieving the many business benefits inherent in electronic records. Although it is intended that all newly created records will be electronic by 2004 there are still likely to be many paper records for many years to come.

6.5.2. In the interim period leading to the full implementation of EDRM, the JSP 700 Series – Information Management Guidance has been produced. The aim of JSP 700 is to assist all MOD staff that use office automation to deliver the greatest business benefit. The JSP contains guidance for managing and sharing electronic documents and records keeping practice in the absence of an EDRMS.

6.5.3. The underlying principle is that staff must ensure that they keep proper records, including e-mails, electronic documents, etc. Unless they use an approved EDRMS, then all electronic documents that need to be retained as records must be printed to paper and be placed on the business unit registered filing system that is managed under extant JSP 441 guidance.

# 6.6 Use of Approved ERM Products

6.6.1. Software packages used to manage electronic records must adhere to the minimum standards specified in the Public Record Office (PRO) Functional Requirements for Electronic Records Management Systems. Only software products that have been approved under the PRO testing scheme for ERMS should be used. (A list of the systems that are currently approved by the PRO can be found at the following URL: http://www.pro.gov.uk/recordsmanagement/eros/invest/listofapprovedsystems.htm - If you cannot access the web page, please seek advice from Info-BCTEDRM1). Other products are unlikely to have the range of facilities required to adequately manage government records.

6.6.2. In the Spring of 2003, an EDRM product and associated services will be available to purchase through the DCSA ICS Catalogue. This product will be implemented in the refurbished MOD Main Building as the interim EDRM solution used prior to the EDRM solution that will be rolled out throughout the MOD on the DII.

# 6.7 Fileplan and Electronic Folder Maintenance

6.7.1. The filing system used for electronic records should closely follow the guidance for paper records defined in Chapter 4. The following paragraphs define the procedures for electronic records referring to Chapter 4 as appropriate.

6.7.2. EDRMS fileplans and associated folders define a hierarchical filing structure into which individual records are filed. The conventional business unit file list and files used in paper filing systems is an ideal top-down structure for analysing the business of a unit into its major components. A good fileplan should be intuitive and should simplify the tasks of deciding where to register a particular document. It should also assist the decisions regarding the review, retention and disposal of folders.

6.7.3. Fileplans are to be constructed in accordance with the guidance in Chapter 4 paragraphs 4.2 and 4.3.

6.7.4. DG Info-Records3 must approve the main headings, numbers and structure of all MOD fileplans before implementation on an EDRMS.

6.7.5. The BRO has responsibility for maintaining the electronic fileplan, although day-to-day maintenance may be delegated to registry staff.

6.7.6. A single fileplan should be used for all records tracked by the EDRMS irrespective of the media (e.g. electronic, paper, optical, film) on which they are held.

6.7.7. The mandatory (if present or applicable) metadata associated with the creation and maintenance of the fileplan is listed in the following table. The meaning and use of these metadata elements is defined in detail at Annex B.

| |
|---|
| Identifier. System ID |
| Identifier. Fileplan ID |
| Title. Title |
| Date. Opened |

| |
|---|
| Date. Closed |
| Aggregation |
| Relation. Has Part |
| Subject. Category |
| Subject. Keyword |
| Security. UK Protective Marking |
| Security. National Caveats |
| Security. Descriptors |
| Disposal. Disposal Schedule ID |

6.7.8. Normally, only an EDRMS Administrator (see section 6.23.5 below ) should be able to open a new electronic folder or folder part. The administrator must ensure that appropriate access controls for the folder are set up; that a disposal schedule is assigned to it; and that an audit trail of events is initiated. The metadata associated with a folder or folder part is defined at section 6.9 below .

6.7.9. Folder parts are to be used to ensure that electronic files remain under management control. Folder parts should be closed when any of the following apply:

a. The folder contains 100 enclosures.

b. The folder has been open for five years.

c. Nothing has been added to the folder for one year.

d. Action on the subject covered by the folder has come to an end.

6.7.10. A new folder part should not be opened unless there is likely to be an immediate need to file new enclosures. The BRO may wish to consider closing the electronic folder altogether if it seems likely that it has no further value. At this point the BRO should ensure that the folder has a valid and appropriate disposal schedule. It should be noted that in exceptional circumstances, i.e. where the disposal recommendation is too short, DG Info Analysis reserves the authority to override any local disposal decisions.

6.7.11. If an electronic folder on an EDRMS contains physical records then the action at section 4.18 for closing registered files also needs to be taken.

6.7.12. When a folder part is closed the BRO must ensure that the following metadata fields (see also section 6.9 below and Annex B for a full description of these metadata elements.) are captured in the folder's metadata:

a. Identifier. System ID

b. Identifier. Fileplan ID

c. Title. Title

d. Date. Opened

e. Date. Closed

f. Disposal. Disposal Schedule ID

g. Disposal. Disposal (due / effective) date

h. Disposal. Disposal authorised by

i. Disposal. Comment (if applicable).

6.7.13. The disposal action has to be authorised by personnel at Pay Band C2 level or above.

6.7.14. The practice of ‘weeding’ electronic folders (i.e. selectively destroying enclosures) is expressly forbidden for the reasons given at section 4.19. Only complete folder parts must be destroyed.

6.7.15. For wholly electronic folders, there is no requirement to maintain Registered File Records Sheets (MOD Form 262A) or Registered File Disposal Forms (MOD Form 262F) where the details of the file’s existence and final disposition are held in the EDRMS metadata.

6.7.16. Records should not normally be transferred between electronic folders unless they have been misfiled. However, all record transfers of this type must be registered on the EDRMS audit log. The audit log should show the date of transfer, record reference and the identities of the source and destination folders.

6.7.17. If after a thorough search an electronic folder part cannot be located, so that effectively the folder has been lost, then this may constitute a breach of security in which case the instructions relating to breaches in JSP 440 must be followed.

# 6.8 Capture of new Records

6.8.1. Capturing records within the electronic environment involves management of the interface between the EDRMS and the applications, such as the word processors or the e-mail clients, which are used to create or receive records. The mechanisms for the capture of records should ensure that:

a. The appropriate records are captured. There should be a clear understanding of the information that should be captured as a record. See section 6.4 above .

b. All types of record are captured. Workable mechanisms should exist for all record-creating applications in use to enable the capture of records from that application according to approved formats and standards. See section 6.15 below .

c. Complete records are captured. Capture mechanisms should be capable of acquiring all the elements that make up a record, for example, an e-mail and its associated attachment, and associating these together in a meaningful and useful manner.

d. The metadata is captured and is associated with records from the time of its creation. This descriptive metadata must be closely bound with the record itself. See section 6.9 below .

e. Links to other records are established and maintained within mixed electronic and paper collections. See section 6.10 below .

# 6.9 Metadata

6.9.1. Metadata is usually defined literally, as ‘***data about data’.*** It is the descriptive information held with a record to enable reliable retrieval and future management. Metadata for normal letters and minutes would typically include title, creator, date created and addressee, however the range of metadata held depends on the type of information in the record. For example, geographical co-ordinates might be essential metadata for a map but totally meaningless for an invoice.

6.9.2. Where properly implemented, metadata provides the information necessary to serve a number of different purposes. Metadata:

· Establishes the provenance of a record, i.e. ‘the context in which the record was created, received and used.

· Indicates whether the records integrity is intact, e.g. it has not been subject to changes after being declared a final record.

· Demonstrates that the links between documents are present.

· Provides an adequate description of the record itself.

· Supports the retrieval of, and access to, the record by a range of users.

· Supports specific functions within the EDRMS.

· Retains contextual information about the record.

· Enables the future interpretation of the historical record.

· Provides essential information to support sustaining the record across time and technological platforms.

6.9.3. At the time of declaring a document as a record, the content and **most** of the applicable metadata is fixed as it is at that point and cannot be changed. There are, however, some metadata elements such as ‘Protective Marking’ and the various disclosability markers that may be amended throughout the life of a record.

6.9.4. Metadata must be stored such that it is clearly and unambiguously attached to the record. The BRO must ensure that the mechanisms within the EDRMS guarantee that metadata cannot become detached from the record content, or lost in some other way, and can always be transferred as a meaningful part of the record when migrating to a new system platform, or transferring into an approved format for permanent preservation (see section 6.21 below ).

6.9.5. In order for the user to enter metadata that will be both useable now and in the future, the BRO must ensure that as many of the metadata elements as possible are generated by the system thus saving the user from having to enter large amounts of metadata for a document or record.

6.9.6. A MOD Metadata standard (MMS) has been developed based on the e-Government Metadata Framework (e-GMF) that has been mandated for use throughout Government. The use of the MMS to establish appropriate metadata capture throughout MOD is a mandatory requirement on all EDRMS implementations.

# Folder Level Metadata

6.9.7. Folder level metadata identifies the attributes that apply to whole groups of records. This metadata serves four main functions of electronic records management:

· Grouping records together – providing an identifying label under which similar records can be grouped together, and which distinguishes separate groups from each other.

· Showing how groups relate to each other – enabling a linking structure that can show the place of one group within the wider semantic structure of the fileplan.

· Enabling management of the group of records as a whole – so that the records can be retained, scheduled and disposed of as a consistent group.

· Enabling access to the group of records as a whole – to demonstrate the narrative context in which records should be understood.

6.9.8. Folder level metadata can also be used to link together conventional paper and electronic filing structures, where these are not in themselves identical, and are an essential element in linking hybrid assemblies where electronic and paper records are contained in one folder.

6.9.9. Folder level metadata must be retained after a folder part has been destroyed for a minimum period of 30 years, to document the action that was taken on the records as part of the formal scheduling process. The proof that a folder part and its contents have been reliably destroyed can be invaluable in answering queries particularly requests raised under DPA and FoI legislation.

6.9.10. The minimum mandatory metadata elements that must be captured at the folder and folder part level are listed in the following table. It should be noted that some of this metadata will be inherited from the fileplan metadata elements. The meaning and use of these metadata elements is defined in detail at Annex B.

| |
|---|
| Creator. Custodian |
| Identifier. System ID |
| Identifier. Fileplan ID |
| Title. Title |
| Date. Opened |
| Date. Closed |
| Relation. Is Part Of |
| Relation. Has Part |
| Subject. Category |
| Subject. Keyword |
| Aggregation |
| Location. Home location |
| Location. Current location |
| Security. UK Protective Marking |
| Security. National caveats |
| Security. Descriptors |
| Security. Username access lists |
| Security. Business group access permission |
| Rights. FOI disclosability indicator |
| Rights. FOI exempt |
| Rights. FOI released |
| Disposal. Disposal Schedule ID |
| Disposal. Disposal action |
| Disposal. Disposal time period |
| Disposal. Disposal event |
| Disposal. Disposal (due/effective) date |
| Disposal. Disposal authorised by |
| Disposal. Export destination |

## Record and Document Level Metadata

6.9.11. Documents and Records need to capture different types of metadata. Document level metadata elements are primarily concerned with identifying the individual document as a single entity i.e. by allocating a title, author and version number. Record level metadata elements are associated with those documents that have been declared as corporate records, and which are necessary to apply full electronic records management controls.

6.9.12. The minimum mandatory metadata that must be captured at the record level is listed in the table below. It should be noted that much of this metadata is either inherited from the upper levels or can be generated by the system.

| |
|---|
| Identifier. System ID |
| Identifier. Fileplan ID |
| Title. Title |
| Creator. Creator |
| Date. Created |
| Date. Acquired |
| Date. Declared |
| Addressee. To |
| Aggregation |
| Type. Document type |
| Relation. Copy [/Pointer] |
| Relation. Has Part |
| Relation. Redaction/Extract |
| Relation. Reason for Redaction/Extract |
| Relation. Rendition |
| Subject. Category |
| Subject. Keyword |
| Security. UK Protective Marking |
| Security. Descriptors |
| Security. National caveat |
| Security. Username access lists |
| Security. Business group access permission |
| Rights. Disclosability to DPA data subject |
| Rights. FOI disclosability indicator |
| Rights. EIR disclosability indicator |
| Rights. FOI exempt |
| Disposal. Disposal Schedule ID |
| Disposal. Disposal action |
| Disposal. Disposal time period |
| Disposal. Disposal event |
| Disposal. External event occurrence |
| Disposal. Disposal (due / effective) date |
| Disposal. Disposal authorised by |
| Disposal. Export destination |

## Mandatory Metadata Elements

6.9.13. To ensure a degree of consistency across MOD and Government and to make certain that records can be exchanged between EDRMS, minimum metadata standards are essential. The following table provides a list of the mandatory record management metadata fields that must be applied to each appropriate document, record or folder. The fields in [square brackets] indicate those additional metadata elements that need to be completed, if applicable, in order to comply with the MOD Metadata Standard (MMS). For more information on the MMS, please contact DG Information, AD Information Management.

6.9.14. Annex B provides a brief definition for each of the mandatory metadata fields listed below, at what level of aggregation they should be applied and a simple example of how they can be used. Diagram 1 above shows the relationship between the different aggregation levels.

| Element | Sub-elements / Refinements | |
|---|---|---|
| | **Mandatory** | Mandatory if Applicable |
| Identifier | **System ID**<br>**Fileplan ID** | [Identifier]<br>[URL]<br>[ISBN]<br>[ISSN] |
| Title | **Title** | [Alternative] |
| Creator | **Creator** | Custodian<br>[Owner]<br>[Contact] |
| Date | **Created**<br>**Acquired**<br>**Declared**<br>**Opened**<br>**Closed** | Cut off<br>[Available]<br>[Issued]<br>[Valid]<br>[Last reviewed]<br>[Modified]<br>[Updating frequency]<br>[Next version due] |
| Aggregation | **Aggregation** | |
| [Subject] | **[Category]**<br>**[Keyword]** | |
| Security | **UK Protective Marking** | Descriptors<br>National Caveats<br>[Non-UK constraint]<br>[Marking change]<br>[Time validity for access control markings]<br>[Codeword]<br>[Nickname]<br>[Business group access permission]<br>[Username access lists] |

| | | |
|---|---|---|
| Rights | **Disclosability to DPA data subject**<br>**EIR disclosability indicator**<br>**FOI disclosability indicator**<br>**[FOI Exempt]**<br>**[FOI Released]** | [Copyright]<br>[Owner]<br>[FOI Released on request]<br>[FOI – Information Class]<br>[FOI – Information Type]<br>[FOI – Organisational Area]<br>[FOI – Cost] |
| Relation | **Is Part Of**<br>**Has Part** | Copy / Pointer<br>Redaction / Extract<br>Reason for Redaction / Extract<br>Rendition |
| Disposal | **Disposal schedule ID**<br>**Disposal action**<br>**Disposal time period**<br>**Disposal event**<br>**Disposal authorised by** | Disposal (due/effective) date<br>Export destination<br>External event occurrence<br>[Review details]<br>[Auto remove date] |
| Location | | Home Location<br>Current Location |
| Addressee | | [To]<br>[CC] |
| [Description] | | [Description]<br>[Table of contents]<br>[Abstract] |
| [Format] | | [Encoding]<br>[Medium]<br>[Extent] |
| [Source] | | [Source] |
| [Status] | | [Version]<br>[Draft]<br>[Purpose]<br>[Approved by] |

| | | |
|---|---|---|
| Type | | Document Type |
| Digital Signature | **Digital Signature** | |
| Preservation | **Originating format** | |

## Optional Metadata Elements

6.9.15. The MMS in not intended to be a comprehensive list of metadata items to be used in the MOD, and the list of potential metadata elements is almost limitless. Therefore before adopting any optional metadata elements, reference must be made to the Defence Data Repository (DDR) to ensure compliance with JSP 329 – Data Management Policy. The following are examples of additional metadata fields that may be applied to meet more specific business requirements:

- Addressee post
- Addressee business unit
- UK Military service staff number
- UK MOD Civil service staff number
- Contract number
- Drawing number
- Map reference code

# 6.10 Management of Physical Records / Hybrid Folders

6.10.1. Active registered files containing paper and other physical media are likely to exist alongside electronic record folders where it is desirable to hold records in non-electronic form. In these circumstances the physical files will not be capable of fully duplicating their electronic equivalent, but their content will augment the electronic version. Together they combine to form hybrid folders.

6.10.2. Where EDRMS is used, it should be used to control records in all forms including those on physical media such as charts, drawing, film reels, microfilm, magnetic tapes, CD ROMs and videocassettes. In order to make best use of the EDRMS ability to track the physical location of items and schedule their review for destruction or further preservation, an appropriate record type (and associated metadata that should include the 'location' element (see section 6.9 above )) must be created.

6.10.3. It should be noted that whilst an EDRMS can fulfil the requirements of a Protective Document Register (PDR), those business units wishing to use the system in this way must contact their relevant security authority for approval prior to implementation.

6.10.4. Hybrid folders are not recommended for the following reasons:

a. Neither the electronic folder nor the physical element of the file will contain all of the pertinent information on their own.

b. Correct enclosure numbering may not be possible in the physical file.

c. Over a period of time, it is likely that the link between the physical file and electronic folder will become blurred.

d. The review process will become more complex.

6.10.5. However where hybrid folders are required it is important that the linking references identifying the two types of record, maintain and display relevant relationships so that the links between an electronic folder and its related paper file are clear to the users and easy to understand. Care must be taken to ensure that both the creators and future users of the data can easily identify this relationship, and that the accompanying metadata is maintained along with the electronic folder and records.

6.10.6. Where a decision is taken to maintain hybrid folders, the following procedures must be followed:

a. Enclosures held in the physical file must be maintained in strict date of origin order and must be allocated sequential enclosure numbers.

b. The physical file must be managed in accordance with the guidance laid down at Chapter 4, paragraph 4.6

c. The metadata associated with the physical file must be declared into the EDRMS to enable tracking.

d. A relationship between the contents of the physical file and the electronic folder must be created in the EDRMS.

e. All enclosures from both the physical file and the electronic folder must be taken into account when decisions are made about the closure of the hybrid folder part.

f. The hybrid folder in its entirety is to be reviewed in line with the instructions in Chapter 5. If the hybrid folder is to be destroyed locally then both elements of the folder should be destroyed. If the folder warrants transfer to DG Info-Records, then both elements of the file should be transferred.

# 6.11 Search Facilities

6.11.1. Once captured into an EDRMS, there is a requirement for users to be able to retrieve the record. The success, or otherwise of a search will depend in part on the type of information stored and its associated metadata. For instance, in a personnel business unit, it may be important for records to be stored with metadata that records a person’s Surname, Service/Staff number and date of birth. Without completing these metadata tags a search for any particular person would be much less likely to retrieve the desired results.

6.11.2. All EDRMS have a range of in-built search capabilities and it is expected that any EDRMS implemented in MOD must have the following search functionality as a minimum. The EDRMS must:

a. Support browsing and navigation of the fileplan structure and allow selection, retrieval and display of electronic folders and their content through this mechanism.

b. Be capable of full-text content searching.

c. Be capable of creating and storing saved searches and making them available to all end users, including those users of other line of business applications.

d. Allow the use of Boolean operands in the construction of a search.

e. Present the search results as a list of folders or records. However it must also indicate to the user if the search yields no results.

f. Not allow a user to have access to folders, records or their metadata, by means of the search and retrieval function, where the access controls and protective markings allocated to those folders or records are intended to prevent access by that user.

g. Support the use of encyclopaedic lists (e.g. a drop down list of record types to search for).

h. Allow a search on metadata field values.

i. Allow other business applications (such as the Enterprise Directory) to execute a search.

# 6.12 Review and Disposal of Electronic Records

6.12.1. The principles of review and disposal, which are described in more detail in Chapter 5, and explained briefly below, should also be followed for electronic records.

6.12.2. Business units, with the exception of ‘Key branches’, have delegated authority to review and destroy locally those records that have no further administrative value and are not considered worthy of permanent preservation. In making such a determination, the following principles should be applied:

a. Local destruction should only be considered for non-policy or ephemeral folders, i.e. those folders that relate to the administration of the business unit. If in doubt, err on the side of caution and forward the material to DG Info-Records with a recommendation that it be considered for permanent preservation.

b. All policy folders are of potential long-term value to MOD and should therefore be considered for forwarding to DG Info-Records with a recommendation that they merit consideration for permanent preservation.

c. Top Secret and Codeword electronic folders cannot be destroyed locally and this material should be forwarded to DG Info-Records, though the recommendation to DG Info-Records may be that they can be destroyed (see section 6.24 below ).

6.12.3. The DIRO must be notified of any electronic folders that are either Top Secret or Codeword so that arrangements for review and transfer can be made.

6.12.4. To assist in the review process, a disposal schedule must be established (see Chapter 5, paragraph 5.3) and implemented on the EDRMS.

6.12.5. Disposal schedules (sometimes called Retention Schedules) are an essential feature of all EDRMS. They ensure that folders are reviewed (usually after a period of years) to determine the appropriate disposal action to be taken on that folder. Each electronic folder must be assigned a schedule. Schedules are normally set when the fileplan is constructed or when a new folder is created. In most EDRMS it is not necessary to define individual schedules for each folder. A range of appropriate schedules can be pre-defined to cover the types of information held and assigned to individual folders as necessary. Schedules can also be assigned to series and hierarchies of folders and inherited as defaults from higher-level folders.

6.12.6. Standard schedules are to be used wherever possible. DG Info-Records can provide advice on the formulation of a suitable set of schedules. An example of a disposal schedule can be found in Chapter 5, Annex B.

6.12.7. Wherever possible, disposal schedules should identify the source of the policy being applied (e.g. Act of Parliament, legal requirement, MOD policy, local administrative purposes, etc.).

6.12.8. Annex A to Chapter 5 gives examples of records likely to warrant permanent preservation.

6.12.9. When an electronic folder is closed in an EDRMS, there is no requirement to raise a MOD Form 262F since the relevant metadata will be held on the system. (A MOD Form 262F will still be required for the physical file part of a hybrid folder.)

6.12.10.The minimum metadata that should be retained, at folder level, on closure of the electronic folder includes:

a. Identifier. System ID

b. Identifier. Fileplan ID

c. Title

d. Date. Opened

e. Date. Closed

f. Disposal. Retention schedule identifier

g. Disposal. Effective date

h. Disposal. Authorized by

i. Disposal. Comment (if applicable).

6.12.11.DG Info-Records will review electronic records considered worthy of permanent preservation following procedures similar to those for paper records at Chapter 5, paragraph 5.1.

# 6.13 Import and Export

## Import from unmanaged environments to an EDRMS

6.13.1. Importing record collections from an unmanaged environment such as shared drives within Windows Explorer to an EDRMS environment will impose a corporate information structure, with appropriate access controls and audit trails on those records. The main advantage of an EDRMS is that once the records have been imported, the system will provide scope for additional metadata to be added regarding the management and status of the record or collection of records. This then is supported by a full audit trail, which will document what actions were undertaken.

6.13.2. Electronic files held in a Windows Explorer environment will possess very little metadata compared with similar documents in an EDRMS. Some new metadata may be added automatically by the importing EDRMS but the manual addition of a full set of metadata to each document may not be feasible. Such documents may have to be imported with a minimal set of metadata. Users may be able to augment this metadata using additional metadata elements and tools available in the EDRMS.

6.13.3. During bulk import of files from the Windows Explorer environment to an EDRMS, there are two methods a business unit can consider:

a. Only those files in the Windows Explorer environment that have been deemed beforehand as being worthy of preservation may be transferred to the record management element of the EDRMS.  At this point, all the relevant metadata, as described in section 6.9 above , will be added to each record in turn.  On completion of the import process, all documents remaining in the Windows Explorer environment should be destroyed.

b.  All files in the Windows Explorer environment may be transferred into the EDRMS as documents with short retention periods.  The relevant owner of each area of the fileplan can then select those documents worthy of retention by registering them as records (e.g.. allocating them to an appropriate folder), whereupon they will acquire metadata establishing the appropriate retention periods and access privileges. Once the retention period of those 'documents' not declared as records takes effect, they can either be retained for a further short period, or destroyed.

## Export of selected electronic folders and files from one EDRMS to another within the same business unit

6.13.4.  Once an EDRMS has been adopted, it may from time to time be necessary to transfer a folder containing records or a series of folders to another EDRMS

6.13.5.  An electronic record is the sum of the document, its context and metadata plus the audit trail to establish provenance. Contextual information and metadata must not be capable of being unlinked from the document therefore the EDRMS export mechanism must include the ability to:

a.  Treat the record as an entity, including context, metadata and audit trail information.

b.  Export a record at any point in its life cycle.

c.  Ensure little or no loss of information.

d.  Enable the audit trail to be annotated noting any changes.

e.  Facilitate the physical transfer of the records.

6.13.6.  Also, as information systems develop, it is likely that records will outlive the EDRMS in which they currently reside.  It is therefore extremely important that the EDRMS has a capability to export, and by implication import information to and from other EDRMS environments.

## Export to another business unit or other government department (OGD)

6.13.7.  Before exporting electronic records from an EDRMS to another business unit or government department the exporting business unit Records Officer must notify DG Info-Records3 and or DG Info-Records1. In these circumstances, because of the possible conflicting business aims of the different business units, there may be variations in the EDRMS metadata.  Close liaison between the importing and exporting business units will be required in order to construct a new record type that will enable the receipt of the incoming records. General advice is laid down in section 4.15 with some more specific additional information detailed below.

6.13.8.  The implementation of the MOD Metadata Standard (MMS) (see section 6.9 above ) to establish the appropriate metadata fields is mandated.

6.13.9.  Prior to exporting the information, all relevant folders should be closed with the metadata amended to provide details of the impending export.  Since all of the relevant metadata will be automatically captured, the completion of a Registered File Record Sheet (MOD Form 262A) and Registered File Disposal Forms (MOD Form 262F) will not be required, however, for audit purposes, the exporting BRO should retain details (a log) of all records that have been exported for 5 years, and the fileplan annotated accordingly (unless of course the business unit is being disbanded). A copy of the log should be copied to the importing BRO who will open the appropriate files in his fileplan.

6.13.10.During the export of records from one EDRMS to another, the BRO must ensure that the metadata for records that may have been previously deleted is also exported to the receiving system.

6.13.11.The imported folders should be closed and stored, with the original fileplan structure preserved, in a separate area of the fileplan from those files already on the system. New folders with different fileplan numbers (Fileplan ID) to those previously imported can then be opened and metadata added to allow them to be cross-referenced with the old folders.  The old folders must not have their fileplan IDs re-numbered to match the new fileplan. The EDRMS audit trail must be set up to capture this export process.

# 6.14 System migration to new computer systems

6.14.1. Migration is the transfer of the contents of an entire fileplan, including all records (and documents) from one hardware and software environment to another. The objective is to preserve the integrity of the records and to ensure they can be retrieved and viewed in the future.

6.14.2. Good practice requires duplicate backup copies. Ideally there should be at least two such copies:

a. A preservation master – from which new working copies can be made.

b. A security master – to guard against catastrophic events such as fire or flood.

6.14.3. Records should be verified when written to new formats, migrated or copied for refresh or backup purposes, and special note made of any loss of data.

6.14.4. The two backup copies should be stored separately from the working versions, preferably off-line with one off-site. If new copies are required, the master should always be returned to the secure store dedicated for its use.

# 6.15 Transfer formats

6.15.1. The formats currently available that meet the requirements defined for transfer, either for export or migration purposes, are PostScript, TIFF, SGML, PDF and delimited file formats (such as comma separated variable). Each of these formats is appropriate for specific record types described in more detailed in the following paragraphs. These transfer formats are robust and are considered to have a long life ahead of them, however conversions should be kept to a minimum because any document format conversion is likely to incur some data loss.

a. Postscript - Any application designed to run on a desktop computer will support Postscript printing.  Since Postscript is designed to be written to file as well as to a printer, it can be used for electronic record transfer.

b. Portable Document Format (PDF) – Adobe PDF is a variety of Postscript and is a universal file format that preserves all the fonts, formatting, graphics, and colour of any source document, regardless of the application and platform used to create it.

c. Tagged Image File Format (TIFF) – TIFF is one of the most popular and flexible of the current public domain raster file formats.  The main strength of TIFF is that it is a highly flexible and platform-independent format that is supported by numerous image-processing applications.

d. Comma Separated Variable (or Value) (CSV) – A CSV file is a way to collect the data from any table so that it can be conveyed as input to another table-oriented application. It contains the values in a table as a series of

ASCII text lines organized so that a comma from the next column's value separates each column value and each row starts a new line. This format is suitable for spreadsheets and small databases.

e. Standard Generalised Mark-up Language (SGML) – SGML is a formal language that can be used to pass information about the component parts of a document to another computer system. Web pages are typically encoded with a set of tags called Hypertext Mark-up Language, or HTML; SGML is the parent language, the tag-set building rules, for HTML and for most other descriptive tag-sets.

6.15.2. To comply with the requirements of the e-Government Interoperability Framework (e-GIF) standard, adoption of Extensible Mark-up Language (XML) as the primary standard for data integration is mandated. XML is the universal format for structured documents and data on the Web. XML is a restricted form of SGML that enables the definition, transmission, validation, and interpretation of data between applications and between organizations.

6.15.3. Metadata describing folder structures, contents and relationships between documents stored in the EDRMS should be transferred with the records, so that the metadata and the links to the document are not broken. The metadata should comply with the minimum mandated in the MOD Metadata Standard.

# 6.16 Security and Access Management

6.16.1. The following paragraphs address confidentiality only in terms of access management and are not intended to replace the department's existing security policy promulgated at JSP 440.

6.16.2. Applying the appropriate level of security to sensitive information is important and in general terms the information owner is responsible for determining its protective marking.

6.16.3. Any protective markings, caveats and descriptors associated with sensitive information should be applied to the information and held on the EDRMS as metadata (see section 6.9 above ).

6.16.4. It is unlikely that EDRMS will be implemented in isolation from other information systems. These systems will make use of existing security services and must follow existing System Security Policies (SSP), and any EDRMS implemented will need to operate within that SSP. Project staff should contact their security authority for advice.

6.16.5. The key characteristics of an effective approach to managing the security and access of records are:

· Authentication – assurance of the identity of an end user, that end users are in fact who they claim to be and that they are the true originators of records to which their names are attached.

· Access control – that a particular user is sanctioned for a particular function, for example, to be able to create a new version of a record, or to alter the filing or retention decisions pertaining to a group of records.

· Confidentiality – ensuring that content access is granted only to those who should have it, and not to those who should not.

· Integrity – evidence that the contents of the record, including metadata and format, have not been altered since the document was declared as a record, as a result of control procedures which would prevent this.

· Non-repudiation of transmission – protection against denial by an individual originating a communication that is stored as a record, as a consequence of assurance gained from the previous four characteristics.

· Non-repudiation of receipt – protection against denial by an individual in receipt of a record.

6.16.6. Working documents that have not been declared as formal corporate records may have access controls placed upon them by their current owners who wish to restrict availability of the document content for various reasons. However, once declared as a record the document comes under corporate ownership and is subject to corporate regulations and procedures.

6.16.7. A feature of EDRMS is its ability to open up access to this corporate information, providing a richer and more accessible information base for the conduct of departmental business. However, there will still be a need to restrict some forms of access to this material e.g. write access to prevent unauthorised changes being made to the existing record, and to restrict all forms of access to defined user groups e.g. to enforce national security, sensitivity and need to know requirements.

6.16.8. All EDRMS provide facilities for the allocation of rights in an access control table, and the attachment of these rights to individual documents, records or collection of records.

6.16.9. The BRO should aim to identify important user groups within the business unit, and allocate broad functional rights to each group. Relevant user groups might include:

- Groups with access to higher levels of protectively marked records.

- Project teams or workgroups.

- Records managers who will manage record collections and metadata.

6.16.10.Functional rights that might be allocated in differing combinations to differing groups might include: Read / retrieval access to metadata or other record descriptions.

- Read / retrieval access to records contents.

- Edit rights to change the content of metadata or record descriptions.

- Read rights to make a physical copy of a record in order to create a new version.

- Records management rights to change any retention or scheduling information.

6.16.11.It should not be possible to edit the contents of a record without creating a new version. Similarly, delete rights (for records, rather than documents) should only be available to the EDRMS administrators.

# 6.17 Cryptography

6.17.1. Definitive guidance on cryptography is available in JSP 440 and JSP 602 – Security of Information. JSP 440 defines cryptography as being the art or science concerning the principles, means and methods for rendering plain text unintelligible, and for converting encrypted messages into an intelligible form.

6.17.2. This definition basically refers to the use of encryption / decryption to safeguard the confidentiality of documents and records, but it is also worth noting that cryptographic techniques are also used for Authentication (e.g. digital signatures) and Integrity (e.g. cryptographic checksums).

6.17.3. Records stored within an EDRMS must be capable of meaningful access in the future. Records that are stored only in their encrypted form will be vulnerable to loss, for all effective purposes, once the means of encryption changes or is replaced. This implies that records should either be:

- Stored in a decrypted form, securely and with the appropriate access restrictions, for future sensitivity review and potential release or selection by the Public Record Office. Or

- Stored with guaranteed access to an historical archive of the means of decryption, which is systematically maintained in conjunction with the records over time; and with metadata which retains the link with the relevant generation of encryption tools and which locates the record within the corporate filing structure.

6.17.4. To avoid the overheads associated with archiving the private encryption key so that encrypted documents can be decrypted even if the user's private key is no longer available, it is recommended that records are stored only in their decrypted form in an EDRMS.

## 6.18 Authenticity and Electronic (Digital) Signatures

6.18.1. A "digitised signature" is a digitised representation of an individual's own hand written signature. "Digitised signatures" are not recommended for use in MOD.

6.18.2. A digital signature is created through a cryptographic process using a private cryptographic key held only by the user and accessed using a Personal Identity Number (PIN) code. The digital signature is a function of the data being signed and the private key. This means that if a digitally signed document is subsequently changed, the signature will no longer verify when cryptographically checked.

6.18.3. Digital signatures are verified using the digital certificate of the signing party. If the signature verifies, it confirms two things:

a. That the document has not been changed since being signed; and

b. That the identity of the signing party is the same as that shown on the certificate.

6.18.4. It is recommended that separate cryptographic key pairs are used for both encryption and signing, however the method in which digitally signed documents are stored is dependent upon the application in use.

6.18.5. In general, a digitally signed document should be stored in the EDRMS in its native unencrypted format along with the signature stating that it has been signed. It is also acceptable to store the certificate of the signer with the signed document to allow faster signature validation.

6.18.6. Should Public Key Infrastructure (PKI) be adopted across MOD, BROs and system administrators will need to be aware that to ensure access to records in the future, distinctions need to be made between:

a. Those applications that use digital signatures but do not encrypt the content of the message hence it may be sufficient to document that the digital signature has been correctly assigned and authenticated, and

b. Those applications that use some form of encryption on the message in order to ensure confidentiality, thus the record becomes inaccessible unless a decrypted version (or the means to obtain one) is available.

## 6.19 Legal admissibility

6.19.1. The Civil Evidence Act 1995, does not specify any special conditions governing the use of computer-derived evidence in court, however, in criminal proceedings, Section 69 of the Police and Criminal Evidence Act 1984 states that any statement produced by a computer will only be admitted into court subject to compliance with certain conditions. One of these conditions provides that "at all material times the computer was operating properly".

6.19.2. It is advised that business units should seek to conform to the provisions of BSI PD0008 - A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (edition 2) (PD 0008). Legal admissibility is significant if the business unit ever needs to use electronic records in legal disputes.

Compliance with PD 0008 cannot assure evidential worth - ultimately this is for the courts to decide – however, non-compliance provides no mechanism to support arguments for evidential worth and without such mechanisms it will be difficult to satisfy the needs of audit. Issues to bear in mind include:

- Are the records complete?
- Are they accurate?
- Are they valid?

6.19.3. The Compliance Workbook for Legal Admissibility of Information Stored on Document Management Systems, PD 0009 is designed to establish the compliance of a document management system with PD 0008. It also enables an audit trail of compliance to be produced that must be stored on the records management application as a record held on the system. When completed, this workbook is the business unit's statement of the extent to which its records management complies with the recommendations in PD 0008.

6.19.4. The establishment of a regular audit of the EDRMS and the ability to easily follow the audit trail are necessary PD 0008 requirements.

# 6.20 Audit

6.20.1. Audits are required for statutory reasons and as part of a business unit's corporate control procedures, especially in those business units where there is a strong requirement for authenticity, such as a contracts or personnel business unit.

6.20.2. The objective of audit is to ensure that appropriate measures are employed to monitor and document operations and any deviations from designated standards and methods of operation. It is important that all of the procedures used to achieve long-term preservation of electronic records are auditable. This means that procedures must be clearly defined and responsibility for their being carried out assigned.

6.20.3. To remain an authentic representation of events, a document, once declared as a record, should not be capable of being changed. Since electronic information is more vulnerable to accidental or deliberate editing, without leaving any traceable evidence within in its own content, the EDRMS must take special measures to prevent retrospective change to corporate records and to record other significant actions taken on them.

6.20.4. After a document has been declared as a record, the ability to edit and make changes to the document should be prevented as the degree to which the authenticity of a record can be demonstrated for legal and accountability purposes will be largely determined by the success of these restrictions. Where it may be necessary to gain update/amend access to maintain the record, to edit the metadata, and take any other action that will modify an attribute of the record, pre-determined procedures and roles should be adhered to and fully documented.

6.20.5. New and related versions of the record can be created by making and editing a copy, and saving this as a new record; for example, it may be appropriate to retain various versions of a document as it passes through draft to finalisation. The EDRMS should be capable of linking together versions of the same record, either automatically by the system or through the use of strict naming conventions, to ensure that the latest version is retrieved by a user search. The user should be aware that earlier versions of the record exist in the system.

6.20.6. An audit trail should be kept recording significant events which have been taken on a record, including the date of the event and identification of the individual responsible. Actions taken should include:

- Any changes which affect the status of the document as a reliable record.

- Any change to the metadata describing the record.

- Copies made of the record to create a new version.

6.20.7. Although it is possible for EDRMS to track all activities relating to the record, including all read and retrieval access, it may not be sensible to do so in all cases. The BRO and systems administrators should give careful thought to the extent that this information will be useful and the long-term use that will be made of accumulating such detailed data. It may be appropriate to restrict this full auditing functionality only to certain categories of record, or to certain groups of users. The more the audit log records, the more it costs in processing overhead. It would therefore be wise to capture the bare minimum events such as record capture, record review, any security breaches and destruction.

6.20.8. Audit activities should be triggered by particular events or on the transfer of records. The information that needs to be gathered and checked against specified criteria will include:

- The process being audited.

- The records being processed.

- The date and time of the event.

- The person responsible for the event.

- Any other relevant comments.

- The transmission and receipt logs.

6.20.9. Audit trails should be provided for all documents. Audit trails should be kept securely, and are available for inspection by authorised internal and external personnel. The audit trails should be capable of being easily followed by auditors who may not have experience of the technologies in use.

# 6.21 Preservation

6.21.1. By definition an EDRMS should preserve records held and prevent the accidental or deliberate modification or deletion of records.

6.21.2. A business unit preservation strategy is required which must address the loss of records due to:

a. The obsolescence of the applications format so that the content cannot be read.

b. Media obsolescence or deterioration.

6.21.3. In addressing these concerns, there are two objectives that the DIRO and systems administrators need to bear in mind.

a. The first is to maintain and preserve the original application programs in which the records were created and held. Where the original application is to be used, it is imperative that the business unit makes provision for an annual review of all applications and platforms to ensure that appropriate support is given for all originating technology. This option is only viable however for the short to medium term. MOD’s preservation strategy insists upon a longer-term preservation, i.e. for periods of seven years and longer.

b. The second is to provide a migration strategy where it will be necessary to ensure that any change to another platform takes account of both the migration requirements of records held in native formats and the requirement to preserve the integrity of the information, i.e. records should be stored together with the contextual metadata in a stable area of the business unit’s workspace to ensure they cannot be modified or deleted by users.

6.21.4. If records are to be preserved in a usable form, consideration needs to be given to the metadata that is required to ensure continued accessibility, and to demonstrate the authenticity and integrity that confers their status as corporate records. In the absence of audit trails, for example, authorship may be unclear and it will be difficult to ascertain the business context of a document. Preservation of documents without their contextual metadata will compromise any preservation strategy.

# 6.22 System Characteristics

6.22.1. Good record management must be made as easy as possible, particularly at the record capture stage. Ideally it should be easier to file properly than not to file (or register) at all, with as few keystrokes as possible required to effect each transaction. The EDRMS should be fully integrated with any Office Automation package in use so that it appears to be a natural extension of the package. For example, it should be possible to register a document directly into the EDRMS from within the word-processor, spreadsheet or mail facilities without the need for a separate 'file' transfer.

6.22.2. Also, the performance of the EDRMS should not slow users down. The EDRMS should be able to display the contents of a record from a search list with as few keystrokes or mouse clicks as possible in as short a period of time as possible. Good industry standards in other respects such as scalability, maintainability, support, help facilities and documentation need also to be considered.

# 6.23 Roles

6.23.1. There are four main groups of users who have some form of responsibility for the implementation of the above policy on electronic records. They are:

- Directorate Records Officers (DIRO).
- Business Unit Records Officers (BRO).
- Systems Administrators.
- End Users.

6.23.2. The role of the DIRO and the BRO are described more fully in Chapter 3, but in the context of an electronic record management environment, additional duties are placed upon them.

6.23.3. *Directorate Records Officers* – manage the business processes or functions within which the records are created or received within the business unit, and determine the length of time the record is retained for operational or administrative purposes. The DIRO must provide personnel within the business unit with a clear distinction between those personal documents that are held at a local level and which have not yet become records, and formal records that should be held in the EDRMS. This should include a clear definition of the transition points through which a personal document becomes a formal part of the record. The DIRO is also responsible for ensuring that:

a. Appropriate electronic records are made of administrative or policy-making activities.

b. All electronic records that are created adequately represent the activity of the business unit.

c. Retention schedules are appropriately allocated by conferring with the BROs.

d. Appropriate backup policies for the records are implemented on the infrastructure on which the EDRMS is implemented.

6.23.4. *Business Unit Records Officers* – are responsible for the management of the information resources, i.e. the records, and in particular for structuring the environment in which the proper capture, maintenance and disposition of records takes place. The BRO should:

a. Participate in the planning of the EDRMS implementation to ensure that records management disciplines are maintained.

b. Ensure that appropriate registration, indexing and retrieval mechanisms exist.

c. Ensure that electronic records are reliable and authentic and that they are preserved (until authorised destruction or transfer) through the use of appropriate audit.

d. Co-ordinate the development of EDRMS procedures for electronic records retention and disposition, and manage the resolution of conflicting requirements.

e. Continue the management of physical records according to their schedule for retention, and ensure the continued migration of electronic records through system changes.

6.23.5. *Systems Administrators (EDRMS only)* – are not only responsible for the design, build and maintenance of information systems but for:

a. Maintaining knowledge about EDRMS functionality, technical operation and processing.

b. Ensuring that the EDRMS is designed and implemented to capture metadata about records to a level consistent with the MOD Metadata Standard, and that this is maintained over time.

c. Implementing technical records management controls to make possible the exchange or sharing of information between business unit across a network.

d. The deletion/destruction of electronic records that are no longer required for transfer or retention and that only they can delete these records from the system.

e. The notification to the DIRO and BROs when a new EDRMS, or enhancements to existing system, are planned where these affect records creation, management access or retention.

6.23.6. *End Users* – comprises those, at all levels of the business unit, who generate and use records in their daily activities. This group is the source of much of the material that constitutes the record. End users are responsible, in the course of their activities, for:

a. Identifying electronic documents that are appropriate for capture as electronic records, because of their business function or content.

b. Creation of electronic records, including the capture of relevant contextual information and metadata describing the record, that is consistent and reliable.

c. Capture of electronic records that authentically document the activities in the course of which they were produced.

d. Initiating the registration of electronic records by the appropriate method.

e. Appropriate use of existing records, and co-operation with any audit trail mechanism.

# 6.24 Forwarding Electronic Records to Director General Information

6.24.1. For the present, records forwarded to DG Info by business units with a recommendation that they be considered for permanent preservation will normally be required in hard copy form (in addition to conventional paper records, records may be forwarded on microfilm or microfiche in some circumstances). In future, it is expected that business units will retain their electronic records on their own EDRMS, only transferring records to DG Info if the business unit no longer has use for the records, but deems that they may have some future potential value to the department or when the unit ceases its function.

6.24.2. Business units wishing to forward records to DG Info in electronic form should, in the first instance, contact Info-BCTEDRM 1 to discuss their requirement.

# 6.25 Director General Information Assistance

6.25.1. Info-BCTEDRM1 can provide advice and assistance with the general application of this Chapter, whilst Info-Records1 and Info-Records3 must approve disposal schedules and fileplans respectively for electronic records. Info-BCTEDRM1 would also be interested to learn of any practical difficulties experienced in applying these instructions that will be updated in light of those experiences.

Home Back to Contents Top of Page Chapter 7 Index

Version 2.0

Last updated 11/03/03

00471 visits since 29.1.03

**JSP 441**

**Defence Records Management Manual Chapter 6 Annex A**

This Page Last Updated:
Friday, 24 January 2003 12:20

✉ Queries, Suggestions, etc.

# MOD Corporate Policy for Electronic Records

## Issue Version 1.0 - March 2002

| | | |
|---|---|---|
| Produced By | [redacted] | Business Change Team |
| Approved by | [redacted] | Director Information Exploitation |

## Introduction

1. This document defines the corporate policy for the management of all existing and planned electronic record collections in the MOD. It sets out the fundamental principles for managing records in electronic form and is aimed primarily at records management staff and those responsible for implementing Electronic Document and Record Management (EDRM) projects.

2. The policy covers records containing all types of information held within MOD at all levels of sensitivity. The terms 'MOD' and 'Department' as used in this document refer to the whole Ministry of Defence, its Agencies and the Armed Forces.

3. The MOD keeps records to support its business and to meet its wider obligations as set out below. Departmental practice and procedures in respect of its records are defined in the Defence Records Management Manual (JSP441) and overseen by the Departmental Records Officer (DRO) under the authority of the DG Information.

4. The importance of good record keeping in large and diverse departments such as the MOD cannot be over-emphasised. It is essential for many reasons:

- Most importantly, to support daily business within the organisation that creates them, but also;
- To support the wider departmental need for information, both outside the originating organisation and in respect of the Department's past activities
- To assist accurate and timely responses to requests under Freedom of Information and Data Protection legislation

- To support MOD compliance with the Public Records Acts
- To enable the Department to respond to legal and quasi-legal cases and justify action taken
- To enable audit.

5. Electronic records have advantages over conventional paper records and enable MOD to:

- Improve the efficiency of business processes that utilise records
- Share information across a wider community
- Have faster and more effective access to information
- Save storage space.

6. At any time there may be several EDRM-related projects and initiatives under way within MOD at many levels: local, sector and centre. This document does not attempt to describe them or relate them to any overall MOD EDRM programme.

7. This document sets out policy for electronic records. Business Units with no form of electronic record management should print copies of electronic documents for use as records in conventional registered paper filing systems in accordance with the Defence Records Management Manual (JSP441).

8. This policy covers:

- the requirements that must be met for the records themselves to be considered as a proper record of activities undertaken by the department and as sufficient evidence to support decisions taken
- the requirements for records systems and processes to ensure the quality and reliability of the records as a valuable corporate information resource
- the use of approved technical solutions
- registration of records
- access to records
- security of records
- authenticity of records
- review of records
- deletion of records
- review of this policy and the quality of its implementation.

9. This policy defines *documents* as **any** tangible information on any medium received or produced by the department and *records* as those *documents* which support some official activity or decision and need to be retained for future reference. It should be noted that although a distinction is made here between *document* and *record* the term *public record* applies to **all** such *documents* and *records* whether held in a recognised records management system or not.

# Fundamental Requirements

10. Electronic records are to be clearly identified and catalogued in a thematically structured file plan following a pattern similar to that given to conventional paper records and described in The Defence Records Management Manual (JSP441). This is fundamental to the proper management and use of records held in any form.

11. Electronic records must be capable of being preserved, stored and reliably and securely retrieved over the required period to satisfy operational, business, legal, statutory, public and national requirements for the information which they contain. The required period of retention will vary according to the nature of that information.

12. Once they are no longer of use to the Department electronic records must EITHER be selected for permanent preservation OR destroyed.

13. Electronic records management systems must at all times ensure that records:

· are present

The information needed to reconstruct activities and transactions that have taken place is recorded

· can be accessed by those entitled

It is possible to locate and access the information and present it in a way that is true to the original presentation of the information

· can be interpreted

A context for the information can be established showing when, where and who created it, how it was used and how it is related to other relevant information

· can be trusted

The information and its representation accurately matches that which was actually created and used, and its integrity and authenticity can be demonstrated beyond reasonable doubt

· can be maintained through time

The record can be deemed to be present and can be accessed, interpreted and trusted for as long as necessary and on transfer to other approved locations, systems and technologies

· can be reliably and securely deleted when no longer required by the Department

Records for which there is clearly no further use must not be allowed to take up valuable storage space and reduce efficiency. Once a record has been officially declared as deleted it must not be reinstated.

14. The maintenance of the evidence of its activities and decisions is an important and necessary function of the MOD. Adequate resources must be applied to the proper management of systems and processes that deal with electronic records to ensure that this task is given its due importance.

15. Electronic records are a highly valuable asset. All systems and processes that handle electronic

records must apply careful controls and strict standards. The sponsors of such systems and processes will be required to:

- identify to DG Information any proposals for new electronic record systems

- identify to DG Information that their systems handle electronic records and provide information to DG Information as required for inclusion in the department's inventory of record collections

- maintain electronic records so that the record nature remains intact

- provide for the transfer of electronic records to other organisations either within or outside the Department.

- keep the records secure and monitor access in accordance with JSP441 and the Defence Manual of Security (JSP440)

- follow any statutory requirements (such as Data Protection, Freedom of Information, the Public Records Acts and copyright legislation) relevant to the electronic records they hold.

- regularly review their records management policy.

# The Transition to Electronic Records

16. While the department is moving towards full electronic working there will be a period during which documents on electronic, paper and other media are held as records. There is a requirement to distinguish clearly whether a particular record is held in the electronic files, the paper files or some other medium.

17. The following policy should be observed:

- Records must be captured

- All records should be electronic as far as possible allowing for legal and practical considerations.

- There should be no unwarranted duplication between the paper and electronic record collections

- All records, whether electronic (on-line or off-line), on paper or any other medium, held by an organisation must be tracked in a single EDRM system which should clearly show where the record is located and in what form it is held.

- DG Information must be advised of all new EDRM projects to assist in maintaining standards across the department.

18. It is essential that organisations planning to implement EDRM contact DG Information and the relevant security authority at an early stage. This is particularly important if highly sensitive material is involved.

# Legal Compliance Obligations

19. It is the responsibility of all authorities in MOD to understand the types of information that are handled and the associated legal and statutory obligations including the requirement to maintain proper records. These obligations apply to records in all forms including electronic records.

20. Legislation can affect record keeping in a number of ways. Some legislation demands that proper records be kept for a defined period (for example the many acts relating to Health & Safety at work). Other legislation may affect the way in which records are protected (for example the Data Protection Acts) or released into the public domain (for example the Public Records Acts and the Freedom of Information Act).

JSP441 specifies best practice in the management of records and will aid compliance with legislation and regulations relevant to the type of information stored.

# Technical Criteria

21. Software packages used to manage electronic records must adhere to the minimum standards specified in the Public Record Office (PRO) *Functional Requirements for Electronic Records Management Systems*. Only software which has been approved under the PRO testing scheme for EDRM should be used.

22. The records management aspects of EDRM must be set up and managed in accordance with the Defence Records Management Manual (JSP441).

# Registration

23. Records must be captured into a thematic structure which facilitates their retrieval and management through time:

- electronic records must be categorised into a file plan comprising files and series of files that have meaningful titles and consistent numerical references
- individuals able to register new records must understand the thematic structure of the file plan and their responsibility for filing new records appropriately
- file plans can cover series with both electronic and paper records if required
- samples of new files and records must be periodically checked to confirm that records have been allocated correctly to the file plan and that meaningful titles have been used
- samples of new files and records must be audited to ensure that the registration system makes sense and records can be reliably found using appropriate search methods. New file plans should be created when necessary.

# Preservation

24. Electronic records offer the possibility of retaining more information than conventional paper form due to the compact nature of the medium and the potential for reducing duplication.

25. Electronic records must be preserved over any change in the supporting infrastructure or holding organisation so that they can still satisfy the original policy requirements. Preservation needs must be satisfied when there are changes in:

- the technology, hardware or software that processes the electronic records and the way records are processed throughout their existence
- the structure of the organisation that creates and manages the records and gives them context
- the definition of terms used in the metadata (ie. the descriptive information held about the records) and within the records themselves
- the categorisation of the electronic records including how the records are grouped and described so that they can be presented in a way consistent with the original understanding of the subject when the record was created.

26. Electronic records which have been transferred to off-line media must still be tracked by the records management system.

# Long Term Preservation

27. Electronic records will normally be held for the whole of their life by the organisation within MOD that created them. This is sensible because the originator is the most likely to need those records and will be best placed to interpret them. Other potential users having a legitimate need may also be given access by the owner. However, as new organisations evolve (usually by division and amalgamation of existing organisations) existing record holdings may need to be transferred to new, appropriate owners.

28. In some cases it may be appropriate to transfer ownership of electronic records to DG Information. There are two circumstances in which this may be required:

- The original owner ceases to exist and there is no obvious successor.
- The records are considered worthy of permanent preservation and are being transferred to the Public Record Office.

# Access Management

29. Access controls are essential to protect sensitive information but should not prevent legitimate access by any authorised parties. Access management should offer a mechanism for opening up information for use outside of the originating organisation.

30. The actual controls used in any particular system will depend on many factors but the general

principles can be summarised as:

- creators and other users or groups should have access to relevant information needed for any legitimate purpose

- electronic records should be made available to provide continuity across changes of staff structure and personnel

- the originator of a record must decide on its sensitivity. This judgement may be on a whole series of files or simply cover individual items. It will identify any restrictions on the records and it will highlight groups or individuals within the organisation who should have or should not have access. Any judgements, including any background reasons for withholding or masking information within the record or record series, should be recorded.

- blanket restrictions on records series should be avoided wherever possible especially if this is only to protect a small minority of records in the series

- records should normally be considered to be part of the 'corporate memory' and access should only be denied where this is necessary because of legislation or sound sensitivity reasons.

# Authenticity

31. Users of records need to have confidence that the records they are using are still true and accurate representations of those records as they were originally filed. However, the degree of trust placed in records can vary. Some records merely act as a simple *aide memoire* with no great importance being placed on their authenticity while others may be crucial evidence to be presented in a court of law. Also, certain records, such as those relating to legal claims and financial transactions, may be the target of deliberate corruption for fraudulent purposes. The degree of authenticity required in an electronic record collection needs to be assessed in each case.

32. The BSI document *A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (BSI DISC PD0008)* defines good practice for the management of electronic records to ensure that authenticity is maintained. All organisations implementing EDRM should seek to comply with the provisions of PD0008.

# Review and Deletion

33. Electronic records considered to be of no further use to the Department and not required for permanent preservation must be deleted as soon as possible, in line with the policy stipulated in JSP 441, to maintain efficiency and conserve space. The following points should be noted:

- Records placed on electronic registered files inherit the disposal metadata of that file and once placed on file individual records should not be weeded

- In common with the practice for paper records, authority to delete electronic records is delegated by the DRO to the organisation which originated those records with the exception of electronic files which contain TOP SECRET and Codeword material on which the DRO must be consulted before deletion in all cases

· Records declared as deleted must not be reinstated. Great care must be exercised when restoring databases from back-up versions to ensure that such deleted records are not reinstated.

# Confidentiality, Integrity and Availability

34. All reasonable measures are to be taken to protect the confidentiality, integrity and availability of electronic records. Once recorded and registered in the system, they must be available and safe from compromise, alteration, misinterpretation or loss.

35. The measures include:

· ensuring adherence to the principles of Confidentiality, Integrity and Availability as laid down in the Defence Manual of Security (JSP440)

· maintaining local policy and procedure for record management appropriate to the type of information held and informing and training staff in that policy and procedure

· training staff to use the records management systems in such a way as to ensure accurate and consistent representation of the records held using appropriate metadata

· auditing the systems to trace any deviation from defined local and departmental policy and procedure

· establishing business continuity plans to ensure a constant service is maintained through any failures or disasters

· strictly managing the access management regime and when necessary enforcing access restrictions and setting user lockouts

· reviewing restrictions placed on access and, where appropriate, relaxing them as soon as possible

· maintaining disaster recovery plans and safeguarding the information from technical failures

· implementing and testing an effective and fool-proof back-up regime including physical protection of back-up media.

# Policy Review

36. The interpretation and implementation of this policy will be monitored to assess its effectiveness and make necessary changes.

37. Monitoring activities will include:

· audit of organisations within MOD to determine their understanding of the policy and their chosen implementation

· extending the policy as necessary to cover emerging areas if these are critical to the creation and use of electronic records

- highlighting non-conformance and tightening controls to improve standards
- agreeing changes and redrafting the policy as necessary.

## Contacts for Further Information

38. For further information on electronic records or related topics contact DG Information's Business Change Team (BCT): [redacted]

Home Back to Contents Back to Chapter 6 Top of Page Index

Last updated 24/01/03

This Page Last Updated:
Friday, 24 January 2003
12:49

Queries, Suggestions, etc.

**JSP 441** Defence Records Management Manual
Chapter 6 Annex B

# Metadata Elements

| Metadata Element | Sub-elements / Refinements | | Definition / Comment<br>Aggregation Level<br>System / User Defined | Example | |
|---|---|---|---|---|---|
| | Mandatory | Mandatory if applicable or present | | | |
| **Identifier** | **System ID** | | The **System ID** is used for the internal purposes of the EDRMS.<br>It is mandatory at **Fileplan**, **Folder**, **Part** and **Record** level.<br>**System defined**. | D01/1651: This is the system identifier that the EDRMS has allocated for this particular record | |
| | **Fileplan ID** | | The **Fileplan ID** is an identifier for a fileplan object.  It is the reference derived from the fileplan itself.<br>It is mandatory at the **Fileplan**, **Folder** and **Part** level.<br>**System defined** (except at the fileplan level). | DG Info/4/2/8/1/2. | |

| | | | | | |
|---|---|---|---|---|---|
| | | Identifier | An unambiguous reference for an object, which distinguishes it from other objects within a given context. | JSP 441 | |
| | | URL | The World Wide Web (WWW) uniform (or universal) resource locator URL and extension that identifies the page or resource. | www.defence.mod.uk/drweb | |
| | | ISBN | For books. | 185554136X | |
| | | ISSN | For magazines or articles there from. | 0010-4532 | |
| **Title** | **Title** | | The meaningful name given to the record. To assist in identification, including for retrieval purposes. Users will often have to specify record titles with a view to their use as a retrieval aid for themselves or for other users.<br>The capture of some documents as records will lead to the population of title fields in record metadata from mapped fields in the document, e.g. email subject lines. If a document does not have a title then a short, informative title must be devised when the document is registered. It is recommended that business units issue guidance for composing titles, for example, ensuring that personnel spell out in full all acronyms and abbreviations.<br>Mandatory at the **Fileplan**, **Folder**, **Part** and **Record** level.<br>**User Defined**. | MOD Record Management Manual | |
| | | Alternative | The alternative name(s) by which the record may be known. | JSP 441 | |

| | | | | | |
|---|---|---|---|---|---|
| **Creator** | **Creator** | | The person, post, team or organisation responsible for the content of the resource (or the person who caused the resource to be brought into the business unit), up to the point of declaration as a record.<br>All values must comply with JSP 457 (Defence Naming and Addressing Manual) and originate from the Enterprise Directory.<br>Mandatory at **Record level** only.<br>**System generated**, however there will be instances where this field will require amendment to some other person who is responsible for the content of the record resource. | The business unit for a publication, the post for official internal correspondence, the person's name for staff-related correspondence. E.g.<br>Organisation - MoD<br>Organisation - DG Info<br>Post - Info BCT EDRM1<br>Person name - [redacted]<br>[Under DII(C), a user's login ID will be their PUIDName, allowing the underlying PUID to be stored as a default. E.g.<br>Country ¬ gb<br>Organisation – Mil<br>Unit – InfoBCT<br>Post – InfoBCT-EDRM1<br>PUID – 1234567890] | |
| | | Owner | The person or organisation that has chief responsibility for the content of the record. | See ‘Creator’ example above | |
| | | Contact | The individual or organisation to be contacted for further information on the content. | See ‘Creator’ example above | |
| | | Custodian | For documents originating outside of MOD, the person who has responsibility for the document within the MOD. | See ‘Creator’ example above | |

| | | | | | |
|---|---|---|---|---|---|
| **Date** | **Created** | | Date (and time [optional]) the resource was created.<br>Applied to the record automatically from the authoring application (e.g. e-mail client) by the EDRMS. If a document bears no date then either its date must be estimated or the date of registration used.<br>Mandatory at **Record level** only.<br>**System generated**. | CCYY/MM/DD (hh:mm:ss) | |
| | **Acquired** | | Mandatory for e-mail, optional for other records but recommended for all externally produced material.<br>Mandatory at **Record level** only.<br>**System generated**. | CCYY/MM/DD (hh:mm:ss) | |
| | **Declared** | | Date (and time [optional]) a document of business activity was declared to be a formal record.<br>One of the principal events in the life of an electronic record without which its integrity and record value is in doubt.<br>Mandatory at **Record level** only.<br>**System generated.** | CCYY/MM/DD (hh:mm:ss). | |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | **Opened** | | Date (and time [optional]) the resource (i.e. the aggregation ‘record collection’) was ‘opened’ and made available for declaring contents.<br>Delineates the ‘start-point’ of the record collection concerned. Records management and business processes are dependent on the availability of a value for this element, e.g. disposal scheduling.<br>Mandatory at **Folder (& part) level** only.<br>**System generated.** | CCYY/MM/DD (hh:mm:ss). | |
| | **Closed** | | Date (and time [optional]) an aggregation (collection) of records was completed and further additions prevented.<br>Defining the ‘end point’ of the records collection concerned. Essential part of managing records lifecycle events (often used to trigger disposal activity through a schedule) and for supporting resource discovery (e.g. the search parameters may include time)<br>Mandatory at **Folder (& part) level** only.<br>**System generated.** | CCYY/MM/DD (hh:mm:ss). | |
| | | Cut off | The regular date on which the folder should be segmented into a new part. | CCYY/MM/DD (hh:mm:ss). | |
| | | Available | The date the information was made available, internally within the organisation, but outside of the area that created it. | CCYY/MM/DD (hh:mm:ss). | |
| | | Issued | The date the resource was made publicly available. | CCYY/MM/DD (hh:mm:ss). | |
| | | Valid | The date range within which the information is valid. | CCYY/MM/DD (hh:mm:ss). | |

| | | | | | |
|---|---|---|---|---|---|
| | | Last reviewed | The date when the information was last verified for its currency by the creator. | CCYY/MM/DD (hh:mm:ss). | |
| | | Modified | The date when the information was last updated. | CCYY/MM/DD (hh:mm:ss). | |
| | | Updating frequency | The time period denoting how often the information is updated. | Daily, weekly, monthly, etc. | |
| | | Next version due | The date the document is due to be superseded. | CCYY/MM/DD (hh:mm:ss). | |
| **Aggregation** | **Aggregation** | | The unit of measurement used to define where in the information hierarchy any records management action is carried out.<br>This element is used to clarify the extent to which actions can be carried out at different levels.<br>Mandatory at the **Fileplan**, **Folder**, **Part** and **Record** level.<br>System generated. | For example, at the folder level, this JSP specifies that the following mandatory metadata will be captured:<br>**Identifier. System ID**<br>**Identifier. Fileplan ID**<br>**Title**<br>**Subject**<br>**Date. Opened**<br>**Date. Closed**<br>**Relation**<br>**Aggregation**<br>**Rights / Security**<br>**Disposal** | |
| **Subject** | **Category** | | The main topic that describes the contents of the information.<br>Mandatory at the **Folder**, **Part** and **Record** level.<br>The terms will be system generated from a controlled MOD Taxonomy. | This element will be automatically mapped to the Government Category List (GCL), e.g. Operations Kosovo – the GCL term is Military Operations. | |

| | | | | | |
|---|---|---|---|---|---|
| | **Keyword** | | Keywords describing the specific subject of the information.<br>Mandatory at the **Folder**, **Part** and **Record** level.<br>The terms will be system generated from a controlled vocabulary or thesaurus. | Allies<br>Kosovo<br>NATO<br>Peacekeeping operations | |
| **Security** | **UK Protective Marking** | | Restrictions and permissions placed on user rights to view records in the EDRMS.<br>Capture of this information in the metadata allows a degree of automation in the protective handling of material in the electronic records environment.<br>Mandatory at the **Fileplan**, **Folder**, **Part** and **Record** level.<br>User generated | TOP SECRET<br>SECRET<br>CONFIDENTIAL<br>RESTRICTED | |
| | | Descriptors | Identifies the nature of sensitive information. | RESTRICTED – **STAFF** | |
| | | National Caveats | Used to provide additional protection of certain types of UK protectively marked material. | UK EYES ONLY.<br>UK EYES DISCRETION. | |
| | | Non UK constraint | For non-UK sourced documents, this element denotes the protective marking and/or constraint that apply. | International Defence Org / Country / Protective marking / Constraint<br>NATO, SECRET, Releasable to PFP | |
| | | Marking change | Describes the UK Protective Marking, the descriptor or National Caveat held previously, the date of change, the authority for the change and contact details. | Protective marking / Date of Change / Post | |

| | | | | | |
|---|---|---|---|---|---|
| | | Time validity for access control markings | Describes the date on which current controls expire or are downgraded. | The format is: Old Marking / New Marking / Date on which change takes place e.g. UK EYES Only, None, 2002-10-16. | |
| | | Codeword | A single word used to provide security cover for reference to a particular protectively marked matter. | Free text | |
| | | Nickname | A nickname is made up of two words selected by the originator and used for convenience for reference to any matter where security protection is not required. | Free text | |
| | | Business group access permission | Group(s) to which access to the information is limited. | PERSONNEL – All personnel managers in MOD. | |
| | | Username access lists | A list of persons including the organisational post title allowed access to the resource. | Post | |
| **Rights** | **Disclosability to DPA data subject** | | Mandatory at the **Folder**, **Part** and **Record** level.<br>User generated | Y / N (default = N) | |
| | **Freedom of Information (FOI) disclosability indicator** | | Mandatory at the **Folder**, **Part** and **Record** level.<br>User generated | Y / N (default = N) | |
| | **Environmental Information Regulations (EIR) disclosability indicator** | | Mandatory at the **Folder**, **Part** and **Record** level.<br>User generated | Y / N (default = N) | |
| | **FOI Exempt** | | Information falls within the scope of one of the absolute exemptions provided for in the FOI Act. | Use one of the absolute exemptions identified in the Act. | |
| | **FOI Released** | | Information published, or due to be published, via the Publication Scheme. | CCYY/MM/DD | |

| | | | | | |
|---|---|---|---|---|---|
| | | Copyright | Identifier or statement indicating the legal ownership and rights regarding use. | Copyright Owner (Copyright statement)<br>e.g. Ministry of Defence, www.crowncopyright.gov.uk | |
| | | Owner | Named individual or organisation which has responsibility for granting access to the information. | Copyright Contact if different to CREATOR. **Contact**. | |
| | | FOI Released on request | Information has been released following consideration in response to a request from a member of the public. | Date of release; who took the decision; whether the entire document or a sanitised version was released. | |
| | | FOI – Information Class | The FOI Act requires ‘Classes of Information’ to be specified in the Publication Scheme. Creators have a responsibility for ensuring that all information within a Class of Information is published. | The agreed MOD list of Classes of Information and supporting topics. | |
| | | FOI – Information Type | The MOD Publication Scheme will also attribute information by ‘type’ e.g. report; speech; policy statement; press release. | The agreed list of Types of Information. | |
| | | FOI – Organisational Area | Information is also organised by reference to ‘Organisational Area’ | The agreed list of Organisational Areas. | |
| | | FOI – Cost | The FOI Act requires Publication Scheme to specify whether there is any change for information. | Cost of public access to the information. £000.00 or ‘No Charge’. | |
| **Relation** | **Is Part Of** | | Identifies instances where the content of a record has a direct relationship with that of another or clarifies how one level of aggregation relates to other levels.<br>Mandatory at the **Fileplan**, **Folder**, **Part** and **Record** level.<br>System Generated. | The purpose of these fields is to establish the relationship in metadata to make it explicit and available for automatic processing. An example includes where a document attachment related to an associated e-mail message. | |
| | **Has Part** | | Mandatory at the **Fileplan**, **Folder**, **Part** and **Record** level.<br>System Generated. | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Copy / Pointer | Mandatory at the **Record** level.<br>System Generated. | | |
| | | Redaction / Extract | Mandatory at the **Record** level.<br>System Generated. | | |
| | | Reason for redaction / extract | Mandatory at the **Record** level.<br>User generated. | | |
| | | Rendition | Mandatory at the **Record** level.<br>System generated. | | |
| **Disposal** | | | Describes what will happen to the records at the end of their lifecycle (sometimes called *sentence* or *retention*), and is used to allow the implementation of retention schedules in the EDRMS.<br>Retention and disposal management is a primary function of EDRMS and essential to compliance with Public Records legislation and the Lord Chancellor's *Code of Practice on the Management of Records* issued under section 46 of the FOI Act 2000.<br>Each sub-element should be viewed as mandatory at the **Folder**, **Part** and **Record** levels.<br>User generated | | |
| | Disposal Schedule ID | | Unique identifier of the disposal schedule that applies to the resource. | D5 | |
| | Disposal Action | | The action to be taken when the disposal condition is reached, i.e. Destroy, Review or Export. | If 'D5' – Retain and destroy 5 years after folder part has been closed. | |
| | Disposal Time period | | Identifies when the disposal action is to be taken. | If 'D5' – Destroy 5 years after folder part has been closed. | |
| | Disposal Event | | The event that may trigger the disposal action. | If 'D5' – Closure of file part will trigger disposal action. | |

| | | | | | |
|---|---|---|---|---|---|
| | Disposal authorised by | | The individual who authorised the disposal of the information. | Person who authorised disposal. | |
| | | Disposal (due/effective) date | May not yet be triggered depending on the disposal rule in force under the schedule in force. | If ‘D5’ – 5 years from file part closure. | |
| | | Export destination | Supports the disposal processes. | If to be exported, the destination of the information. | |
| | | External event occurrence | The external event that may trigger the disposal action. | Business activity on the folder may have ceased. | |
| | | Review | Date on which the resource should be reviewed to determine its business/historical value. | CCYY/MM/DD | |
| | | Conditions | A specific period of time following a specific event determining the period for which the information must be kept for business purposes. | CCYY/MM/DD | |
| | | Review details | Details of reviewers and any review decision taken. | Free text | |
| **Location** [Mandatory for physical formats.] | | Current Location | Defines the current physical location of an object / information and enables the tracking of its location.<br>User generated. | Current Location: Parliamentary Branch | |
| | | Home Location | Defines the normal physical location of an object / information.<br>This element is best implemented at the Fileplan level, enabling the records to inherit this metadata field. | Home Location: DG Info Library, Room 820, St. Giles Court – Shelf Ref.: HH632 | |

| | | | | | |
|---|---|---|---|---|---|
| **Addressee** | | To | The person (or persons) to whom the record was addressed.<br>Intended recipients should be captured automatically on point of declaration to the system.<br>Mandatory at **Record level** only.<br>System generated. | E-mail address | |
| | | CC | The person (or persons) to whom a courtesy copy of the record was addressed. | E-mail address | |
| **Description** | | Description | Free text explanation of the information.<br>This element provides additional detail that may be more helpful to some users that Title, Fileplan ID, Subject, etc.<br>Optional at the **Fileplan**, **Folder**, **Part** and **Record** level. | Free text description. | |
| | | Table of contents | Copy of the table of contents of main headings or sub-sections in a document. | Useful for reports.  Highly desirable for books. | |
| | | Abstract | A summary of the record contents or other notes. | Abstract or Précis of record contents. | |
| **Format** | | Encoding | The coding of IT formatted items.<br>Mandatory at the **Record** level for all refinements.<br>System generated. | Text, html. | |

| | | | | | |
|---|---|---|---|---|---|
| | | Medium | The material or physical carrier of the information.<br>User generated. | Book, VHS videotape, CD Rom, IT File or folder. | |
| | | Extent | The size or duration of the item.<br>System / User generated. | 178 pages, 198kb., 3 hours. | |
| **Source** | | Source | A reference to information from which the present information is derived.<br>Should only be used when one or more RELATION fields cannot be used. | Free text field describing the source. | |
| **Status** | | Version | Version of the document. All versions of the same document will have the same title and identifier.<br>Mandatory at the **Document** level.<br>User generated. | Free text identifier, normally a number, where integers denote formal issues of documents. | |
| | | Draft | Indicates if the document is still at draft stage.<br>Mandatory at the **Document** level.<br>User generated. | 'Yes' or 'No' | |
| | | Purpose | Indicates the purpose or use of the information.<br>Mandatory at the **Document** level.<br>User generated. | Free text field, e.g. 'Version for consideration by the Information Management Metadata Reference Group.' | |

| | | | | | |
|---|---|---|---|---|---|
| | | Approved by | Used to indicate where a person or group within MOD has formally approved a document.<br>Mandatory at the **Document** level.<br>User generated. | Person / Group i.e.<br>[redacted] DG Info | |
| **Type** | | Document type | Type of record that in some respect displays different behaviour from that expected in the default type.<br>This requirement envisages the need for Data Protection Act (DPA) compliance<br>Mandatory at the **Record** level.<br>User defined. | The personal file for a civil servant will require retention for up to 100 years for superannuation purposes. Annual appraisals, leave records, etc. will form part of this record and contain personal data, but have a more limited useful life and their behaviour in terms of retention needs to follow a different rule from that of the rest of the file. | |
| **Digital Signature** | **Digital Signature** | | The Public Record Office will examine what metadata is likely to be created by digital signature technology and how far it is of relevance in records management when the adoption of this technology is further advanced in UK government. Further additions will be made to this element when this work is completed. | | |

| | | | | | |
|---|---|---|---|---|---|
| **Preservation** | *- This element is subject to further development as a result of the definition of sustainability requirements for material retained in departments for extended periods of time. -* | | Information on the migration, sustainability and preservation management processes that have been employed during the life of the record (and its component(s)), to facilitate its survival across technical platforms.<br>This element is used to support departmental migration activity, sustainability and archival preservation of the record and preserve aspects of the provenance of the record across transfer of custody between the departments and to the Public Record Office.<br>[Mandated for records identified as for permanent preservation or as required to be sustained for business purposes periods in excess of circa 7 years.]<br>This element is expected to be system generated from individual components at record capture stage. | | |
| | | Originating Format | Mandatory at the **Record** level.<br>System Generated. | Microsoft Word 97 | |

Home Back to Contents Back to Chapter 6 Top of Page Index

Last updated 24/01/03

This Page Last Updated: Wednesday, 05 March 2003 11:13

Queries, Suggestions, etc.

JSP 441

Defence Records Management Manual Chapter 7

# Film, Video and Photographs

## 7.1 Film and Video Records

7.1.1 Films/videos may range from full productions, such as public relations and training films, to records of tests, trials, operations, reconnaissance etc. They may be edited or unedited and of any duration. They may or may not bear a protective marking.

7.1.2 Each year, any business unit responsible for making or sponsoring a film/video in the preceding year is to forward details to DG Info-Records1, who will, in turn, liaise with the Public Record Office to identify films which appear to warrant permanent preservation. Selected films/videos will be transferred to the Imperial War Museum - IWM - (for subjects primarily of military interest) or the National Film and Television Archive - NFTA - (for other subjects).

## 7.2 When to Transfer Film or Video Records

7.2.1 Selected master copies should be forwarded to the IWM or NFTA as soon as possible after their selection has been confirmed by DG Info-Records1 and not later than 10 years after their creation. DG Info-Records1 will confirm the appropriate recipient of selected material.

## 7.3 What should be Transferred

7.3.1 In the case of film, a master copy will be either the original negative or a good quality duplicate negative, fine grain positive etc. In the case of video, a master copy will be either the original tape or a broadcast standard duplicate.

7.3.2 A viewing copy of the film should be transferred with the master. When a film is produced in different versions it is important to forward both a master and viewing copy of each version.

7.3.3 Film transferred to the Imperial War Museum must be accompanied by any documents relating to its production e.g. scripts, shotlists etc as well as posters and training notes.

## 7.4 Films or Videos which do not merit preservation

7.4.1 Films/ videos not required for preservation are to be destroyed when they are no longer needed for official purposes (but see para 7.9). DG Info-Records must be advised in writing of any case in which the material is still required by the business unit 25 years after its creation.

## 7.5 Warning Concerning Films pre-dating 1952

**7.5.1 Any business unit retaining 35mm film appearing to date from 1952 or earlier should isolate the film and, as a matter of urgency, contact the Film Department of the Imperial War museum (0171-416 5000) for advice. Such film is likely to have been printed on cellulose nitrate stock and constitute a very serious fire hazard.**

## 7.6 Still Photographs

7.6.1 Each MOD business unit holding still photographs is responsible for deciding whether they are of sufficient historical interest to merit permanent preservation. To assist in this task, the following guidelines should be used:

- 
- **Age of material**. Photographs should normally be retained for 5 years before they are considered;
- **Quantity**. Only a small selection of the annual output should be transferred. As a rule, no more than 200 photographs;
- **Subject matter**. Subjects likely to warrant preservation include exercises, new equipment, senior personnel or material related to a major incident;
- **What to transfer**. Both a negative and a print should be forwarded. Both colour and black and white is acceptable. All photographs should be accompanied by some kind of supporting documentation.

7.6.2 it should be noted that these instructions do not apply to photographs which form an integral part of a registered file. Such photographs are not to be removed from the file which is to be reviewed in the normal way.

## 7.7 Photographs which do not merit preservation

7.7.1 Photographs which do not merit permanent preservation should be destroyed when they are no longer needed for official purposes (but see para 7.9). DG Info-Records must be advised in writing of any case in which the material is still required by the business unit 25 years after its creation.

## 7.8 Where to send Photographs

7.8.1 Photographs selected for preservation should be forwarded to the Imperial War Museum after contact has been made to arrange the transfer. The contact point is:

**The Keeper**
**Department of Photographs**
**Imperial War Museum**
**Lambeth Road**
**London SE21 6HZ**

**Tel: 020 7416 5000**

## 7.9 Service Museums

7.9.1 If, exceptionally, it is felt that surplus film, video or photographs not worthy of preservation by the Imperial War Museum may, nevertheless, be of value to a Service museum full written details of the nature of the material concerned must be forwarded to DG Info-Records1. If appropriate, DG Info-Records1 will seek approval from the Lord Chancellor for the "presentation" of the material to the relevant museum.

Home Back to Contents Top of Page Chapter 8 Index

Last updated 05/03/03

This Page Last Updated:
Friday, 11 October 2002 12:45

Queries, Suggestions, etc.

**JSP 441** **Defence Records Management Manual Chapter 7 Annex A**

# Microform Records

**(i)** The term microform includes microfilm, microfiche and other similar formats, such as aperture cards, jacketed fiche and blipped film.

**(ii)** As far as possible microform records should be passed to DG Info-Records in the original negative form along with a silver nitrate copy and should conform to BS 5699.

**(iii)** The following storage conditions are recommended:

- temperature 16C to 2OC
- relative humidity:
  - Acetate 15 to 40%
    Polyester 30 to 40%

Rapid changes in environmental conditions should be avoided.

**(iv)** At present the Public Record Office is able to accept only two microform types:

- 35 mm microfilm
- 100 frame microfiche

If records which are being recommended for permanent preservation are not in either of the above two formats, the original records (if they have survived) should not be destroyed and DG Info(Exp)-Records1 should be contacted for advice.

**(v)** There may be occasions when only part of a microfilm or microfiche might be worthy of permanent preservation (for example, where a microfilm consists of copies of a number of registered files). In those circumstances, however, the whole film or fiche should be forwarded with a covering note identifying the files which are recommended for permanent preservation.

**(vi)** To enable individual documents to be identified, each microfilm and microfiche must have some indication of its contents and each frame must be numbered (foliated).

**(vii)** Contents are most conveniently indicated by a title frame at the beginning of each film, or part of a film, and at the first frame of a fiche (top left hand corner) and this should be carried out as normal practice during initial filming operations.

**(viii)** If you require further advice regarding microform records please contact Head of DG Info-Records1.

Home | Back to Contents | Back to Chapter 7 | Top of Page | Index

Last updated 11/10/02

This Page Last Updated:
Wednesday, 05 March 2003 11:13

Queries, Suggestions, etc.

JSP 441

Defence Records Management Manual
Chapter 7 Annex B

# Disposal Arrangements – MOD Security -Sensitive Image Records selected for Preservation

(i) Within the scope of the Public Records Act 1958, material may be selected for preservation either as deposited records under Section 4(1) of the Act, or as records to be presented under Section 3(6).

(ii) MOD's policy is that imagery selection should occur five years after creation. The result of this process is normally that video*/photographs, of a military nature, selected for the national archive are deposited at the Imperial War Museum (IWM), while those of more limited or predominantly local interest may be presented to an appropriate institution.

[Note: the term "video" is used to describe moving film in both cine and video-cassette format]

(iii) Records selected for preservation but which still merit a security protective marking cannot normally be transferred to the place of deposit/presentation until the need for that marking ceases.

Procedure for video/photographs, still sensitive, selected for deposit or presentation

(iv) Material must be packaged within boxes of archival standard.

(v) Within the box, photographs (whether negative or print) must be individually enclosed within photographic envelopes, each envelope marked with an identifying number or text.

(vi) Individual videos must be marked likewise, on the video-sleeve/box and also on the video cassette/cine-reel itself.

(vii) Within each archive box must be placed a consignment instruction giving the following:

- a hardcopy list identifying the contents by subject (also by serial number if appropriate)
- the review decision for each item (i.e. deposit or presentation)
- the institution selected to receive it
- the recommended year of its next sensitivity review - no more than 10 years ahead
- a brief explanation of its current sensitivity

- signature, name and position of reviewing officer, and the date

(viii) The archive box must be marked externally with the following:

- "Image records for sensitivity re-review"
- the source of the imagery (e.g. "DERA Farnborough")
- the earliest recommended review year on the consignment instruction
- the highest protective marking applicable to the contents

(ix) A second copy of the consignment instruction must accompany the archive box.

(x) Finally, the archive box must be sent, in accordance with appropriate JSP 440 procedures, to:

[redacted]

Deputy Departmental Records Officer
Ministry of Defence
Room 012, Old War Office Building
London SW1

Conflict between business use and archival preservation

(xi) Usually, business use of image records has lapsed after five years. If it has not and the video/photograph is selected for preservation, a copy must be created. The copy will be retained locally, clearly marked "Copy - destroy when business value ceases; original has been selected for preservation at <name of chosen institution>". The original will be despatched via the above procedures.

Home Back to Contents Back to Chapter 7 Top of Page Index

Last updated 05/03/03

**This Page Last Updated:**
**Monday, 20 January 2003 12:08**

Queries, Suggestions, etc.

**JSP 441** **Defence Records Management Manual Chapter 8**

# Forwarding Records to DG Info-Records

## 8.1 When to Forward Records to DG Info-Records

8.1.1 Having identified records which are worthy of consideration by DG Info-Records for permanent preservation, in accordance with the guidelines in Chapter 5, the timing of their passage to DG Info-Records will be governed by a number of factors.

8.1.2 Records held by MOD HQ and other civilian business units should normally be forwarded to DG Info-Records within 5 years of their closure unless the business unit has identified an ongoing administrative need to retain the records locally. Where this is the case the records may be retained for an extended period however **they must be forwarded to DG Info-Records within 25 years of their closure unless prior written authority has been obtained from Head of DG Info-Records to retain them**.

8.1.3 Records held by Service HQs, formations and units may be retained locally for up to 25 years after their closure though they may be forwarded to DG Info-Records at any time in the intervening period if they have ceased to have administrative value but merit consideration for permanent preservation. DG Info-Records 2e should be contacted before unregistered records are forwarded, unless they form part of a "rolling" arrangement. **No records should be retained for longer than 25 years without the written approval of Head of DG Info-Records.**

**8.1.4 If you plan to send a large quantity of records to DG Info-Records please contact us first to appraise us of the type and quantity of records involved. This will ensure that suitable provision can be made for their arrival.**

## 8.2 Closure of Business Units

8.2.1 When a branch is due to be closed (or a ship decommissioned) the administrative authority must include detailed instructions which make provision for the appropriate disposal of the records held by that branch. If records are to be transferred to another branch action should be taken in accordance with Chapter 4, para 4.15. Records which are not to be transferred to another business unit but nonetheless appear to warrant permanent preservation, or to have long term administrative value, should be forwarded to the administrative authority for appropriate action. Where this is not practical advice should be sought from DG Info-Records 2.

## 8.3 Scientific and Technical Reports

8.3.1 Business units which create or sponsor scientific and technical reports and similar documents should include DG Info-Records 2 on the distribution list when the reports are issued. They will be retained and, at a later date, considered for permanent preservation. They will be held in secure conditions and only the originating business unit will have access to them.

## 8.4 Sponsors of Manuals and Books of Reference

8.4.1 Books of reference, manuals, directories etc are to be considered by DG Info-Records for permanent preservation. Sponsors of such material must ensure that when the publication becomes obsolete or is superseded a copy is forwarded to DG Info-Records 2e in accordance with the instructions in Chapter 5, para 5.10.1.

## 8.5 Review of Records by DG Info-Records

8.5.1 Records which have been received by DG Info-Records are first reviewed 5 years after their closure. At this time a reviewer will examine the record and assess its potential historical value, taking into account the recommendation made on the Registered File Disposal Form (MOD Form 262F) by the originating business unit (see Chapter 5 para 5.5). Records which are deemed to have historical value will be stored and reviewed again some 20 years later. During this second review the historical value of the records is reassessed. The passage of time between the creation of the records and this second assessment allows the reviewer to make a better judgement about their historical significance and value and also to assess whether the material remains sensitive.

8.5.2 DG Info-Records works closely with an Inspection and Documentation Officer (IDO) from the Public Record Office (PRO) who liaises with the team of MOD reviewers to ensure that suitable material is selected for transfer to the PRO.

## 8.6 Transfer of Records to the Public Record Office

8.6.1 Records which are ultimately identified as worthy of permanent preservation are then passed to the listings section of DG Info-Records where they are prepared for transfer to the PRO. This involves assigning them to an appropriate PRO "class" (the term used by the PRO to categorise different types of record) and allocating an individual reference number. Records are then normally transferred to the PRO and released to the public 30 years after their creation (or in the case of registered files, 30 years after their closure).

8.6.2 The Public Records Act makes provision for the continued closure of some records which are identified as being too sensitive to release after 30 years. This may be on the grounds of national security or personal sensitivity. Such records can remain closed for an extended period, either held by the PRO or retained by MOD. However, the Lord Chancellor's approval must be sought and it is therefore imperative that records which might warrant continued closure are identified to DG Info-Records within 25 years of their creation/closure. Any business unit holding records in this category should write to Head of DG Info-Records who will provide specific guidance.

## 8.7 Sending Records to DG Info-Records

8.7.1 There is more than one destination for records being forwarded to DG Info-Records. The appropriate destination is determined by the type of record involved. Listed below are details of the different types of records generated by business units and the appropriate place to send them:

| Originator | Type of Record | Send to: |
|---|---|---|
| All | Registered files (other than TOP SECRET and Codeword and files containing Atomic and Nuclear records) | DG Info-Records 2e2<br>Bourne Avenue<br>Hayes<br>Middx UB3 1RF<br>Tel: 396 HB<br>(020 8573 3831 x 396) |
| All | TOP SECRET and Codeword files and records | DG Info-Records lc<br>Room 012<br>Old War Office<br>Whitehall<br>London SW1A 2EU<br>Tel: 78496 MB<br>(020 7218 8496) |
| All | Atomic and Nuclear records | DG Info-Records lc<br>Room 012<br>Old War Office<br>Whitehall<br>London SW1A 2EU<br>Tel: 78496 MB<br>(020 7218 8496) |
| All | Civilian personnel records | DSDC(L)4b<br>Llanelli<br>Dyfed SA14 8YP<br>Tel: 351 LC<br>(01554 822351) |
| All | All other records | DG Info-Records 2e2<br>Bourne Avenue<br>Hayes<br>Tel: 020 8573 3831 x 332/323 |

| | | |
|---|---|---|
| Certain Air Force Department Files (see Chapter 5, para 5.1.3) | TOP SECRET, Codeword and Atomic | AHB1 (RAF)<br>266/U4<br>RAF Bentley Priory<br>Stanmore<br>Middx, HA7 3HH<br>Tel: 7825 BP<br>(020 838 7000 x 7825) |
| As above | Other AFD files | AHB4 (RAF)<br>266/G4<br>RAF Bentley Priory<br>Stanmore<br>Middx, HA7 3HH<br>Tel: 7315 BP<br>(020 838 7000 x 7315) |

## 8.8 Retrieval of Records from DG Info-Records

8.8.1 if there is a need to consult records which have been submitted to DG Info-Records originating business units can request their temporary return using **MOD Form 262E** (Requisition Form). In the case of records held at Hayes the requisition should be forwarded to DG Info-Records 2e2. In the case of urgent requisitions the MOD Form 262E may be faxed to DG Info-Records 2. The fax number is 0181 569 2751. In the case of records held at Old War Office, requisitions should be sent to DG Info-Records 1c.

8.8.2 Records will not be forwarded to business units other than the originating business unit (or the business unit now responsible for the records).

8.8.3 Closed records recovered from the archives must not be added to or altered in any way and must be returned to DG Info-Records as soon as they are no longer required.

## 8.9 Sending Unregistered Records to DG Info-Records

8.9.1 Unregistered records (e.g. records not on registered files) might include maps, plans, drawings, and charts. Such records should be reviewed in the same way as registered files to determine whether they merit consideration by DG Info-Records for permanent preservation (see Chapter 4, para 4.21 and Chapter 5, para 5.8). Where they merit such consideration they should be forwarded as outlined below.

8.9.2 Such records should, wherever possible, be placed in standard archive boxes DG Info-Records 2 can advise on their procurement), though bound volumes may be sent unboxed. Each box or package is to be accompanied by a list of its contents, in duplicate. The highest classification of the enclosed material, the year of its origin and the reason that its permanent preservation is being recommended must also be indicated.

Home Back to Contents Top of Page Chapter 9 Index

**This Page Last Updated:**
**Monday, 20 January 2003 12:08**

Queries, Suggestions, etc.

**JSP 441**

**Defence Records Management Manual Chapter 9**

# Public Access to Records less than 30 years old

## 9.1 Criteria for Access

9.1.1 Access to records which are not yet 30 years old, whether in the Public Record Office (PRO) or held by MOD, is granted at the discretion of the government department to which the records belong. The Open Government Initiatives, including the White Paper on Open Government published in July 1993 and the Code of Practice on Access to Government Information, do not affect departmental discretion. They do, however, seek to reduce the amount of material which is closed for longer than 30 years and make provision for more records to be released by:

- use of more exacting criteria to justify continued closure;
- re-review of previously withheld information;
- identification of material which is less than 30 years old but may be suitable for accelerated release;
- response to ad hoc requests.

9.1.2 In addition, information and, in certain circumstances, documents, can be made available in response to requests under the Code of Practice on Access to Government Information.

9.1.3 The guiding principle in these initiatives is to make as much as possible of the original record available to the public. On receipt of requests for access to material before it is 30 years old MOD is required to consider whether the material is suitable for early release. If it is the Lord Chancellor's approval must be sought. If it is not suitable for release, or resources are not available for the process of transfer to the PRO, MOD must consider whether granting access can be justified and defended as being in the public interest.

## 9.2 Sponsored Access

9.2.1 "Privileged access", meaning the granting of special access to selected individuals, is inconsistent with the spirit of open government. Access by individuals should therefore only normally be approved if the individual is involved in research which is commissioned, sponsored or approved by MOD or is seen to be research from which HMG or MOD will derive benefit, and can be justified as being in the public interest. Such "sponsored access' can be agreed at the discretion of the business unit holding the records concerned.

9.2.2 Such access should only be approved if the work involved in making the appropriate records available does not detract significantly from the ongoing work of the business unit.

9.2.3 In cases of doubt about the merit of allowing sponsored access, or for more detailed advice on the subject, please contact DG Info-Records1.

Home Back to Contents Top of Page Index

Last updated 20/01/03

This Page Last Updated: Tuesday, 11 March 2003 12:58

# JSP 441

# Defence Records Management Manual

Queries, Suggestions, etc.

# Index

A B C D E F H I M N P R S T U V W

Home Back to Contents Top of Page

# JSP 441

# Defence Records Management Manual

**Version 3**

# June 2007

**DG Information**
**Corporate Memory**

| | | |
|---|---|---|
| PRODUCED BY | Info-CMemERM<br>and<br>Info-CMemR | CORPORATE MEMORY |
| APPROVED BY | Info-CMem DD | HEAD OF CORPORATE MEMORY |

## CONTENTS

# Foreword

## About this Manual

The contents of the manual are intended for all MOD staff, military and civilian. Where there are legitimate differences in procedure these are made clear but, in the main, the procedures are intended to apply to all. The content of this manual sets out MOD records management policy and defines the following areas:

a. It defines our legal obligations and sets out our statutory obligations under the Public Records Acts of 1958 and 1967.

b. It defines the policy which applies throughout MOD, i.e. within MOD HQ and other civilian branches as well as Service formations and units and Defence Agencies. Where the regulations governing different parts of MOD vary this is made clear.

c. It explains how the task of managing the records we produce is co-ordinated, and identifies the role and responsibilities of branches

d. It identifies effective methods of storing information in a coherent manner and of reviewing and disposing of information in an efficient and cost effective way.

NOTE: The term 'branch" is used for convenience as a reference to each part of a Directorate or Service formation which maintains a discrete file list and which is responsible for the opening, closing and reviewing of files. Civilian ranks are also used for convenience and should be taken to equate to their Service equivalent where appropriate.

## Equality and Diversity

This policy has been assessed for Equality and Diversity Impact in accordance with the Department’s Equality and Diversity Impact Assessment Tool, and a full impact assessment undertaken.

# Chapter 1

## Underpinning Legislation

### 1.1 Background

The public records of the United Kingdom date back to the 11th century and form a rich archive which is a part of our national heritage. The great wealth of documents and other records stored at The National Archives (TNA), located at Kew, have led to its recognition as one of the most significant archives in the world.

### 1.2 The Public Records Act 1958 & 1967

The law on public records is set out in the Public Records Acts of 1958 and 1967. Public records are defined in the Acts as "administrative and departmental records belonging to Her Majesty's Government, whether in the United Kingdom or elsewhere". These include electronic and paper records, photographic material, film, video, audio, and samples and models which have been made for the purpose of conveying and recording information.

The Public Records Act of 1958 places a responsibility on all government departments to review the records which are generated within the department, to select those which are worthy of permanent preservation and transfer them to TNA, and to destroy all records which are not selected. The 1958 Act stipulated that all surviving public records should normally be released to the public 50 years after their creation; the Public Records Act 1967 reduced that period to 30 years.

There are exceptions to the 30 year release rule, usually on the grounds of an ongoing administrative requirement or continued sensitivity. However, all such exceptions need to be approved by the Lord Chancellor who is the Minister responsible for public records. It is also permissible for records to be held in places other than TNA (known as "approved places of deposit") with the Lord Chancellor's approval. However, with the introduction of the Freedom of Information (FOI) legislation, files transferred to TNA are released on transfer unless an FOI exemption is claimed prior to transfer.

### 1.3 The Freedom of Information Act 2000

The Freedom of Information (FOI) Act 2000 provides a statutory right of access to information held by public authorities. The Act also requires that information can be considered for release proactively though the Publication Scheme. Top Level Budget (TLB) FOI Focal Points constitute a centre of FOI expertise within the TLB area and form the core of a network for efficient pan-MOD handling of requests for information. The MOD policy lead on issues relating to openness, including implementation of the FOI Act rests within Director General Information (DG Info).

All public authorities are required to comply with the FOI Act, which came into effect from January 2005. The FOI Act applies to all parts of MOD including the Armed Forces, Agencies and Trading Funds, whether they are located in the UK or overseas. Only the Special Forces and any units actively providing assistance to the Security and Intelligence Agencies are outside of its scope.

Lead responsibility for MOD FOI policy rests with DG Info. A great deal of information, including the answers to some Frequently Asked Questions, is available on the OPSI (Office of Public Sector Information) Website.

The requirement to maintain a Publication Scheme is unique to the UK's FOI legislation. The objective is to encourage the proactive and continuous disclosure of information on topics of public interest. In practice, "publication" means making information reasonably accessible, and in most cases this is likely to be achieved by placing the information on an Internet site.

The Act says that public authorities must specify Classes of Information they intend to publish, say how this information will be made available and whether it will be available free or on payment. The Publication Scheme can be seen as a catalogue of the information MOD makes available. In practice, the intention is to provide a direct link from the Publication Scheme to any information that is published on the Internet.

### 1.4 The Data Protection Act 1998

The Data Protection Act (DPA) 1998 is the result of a European Directive on Data Protection, which requires Member States to "protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data". All Service and civilian members of staff are bound by its provisions, which confer certain rights and responsibilities. The Act applies to all parts of the UK.

The DPA is about access by individuals to personal data held on them by any organisation whereas the FOI Act relates to the disclosure of information held by public authorities. Responsibility for ensuring the implementation of the DPA throughout MOD lies with DG Info. For more information about the implications of the DPA please refer to the DPA Intranet page and also JSP 440: Disclosure of Information.

### 1.5 What Are Public Records?

All documents generated by Government Departments are legally Public Records as covered by the terms of the Public Records Acts.

This does not however mean that all documents will be worthy of permanent preservation. The task of each department is to select those documents which merit permanent preservation and to safeguard them accordingly. Subsequently decisions must be made about the length of time for which records should be retained taking into account such issues as legal or contractual requirements.

Once the administrative need to retain a record has ceased a decision needs to be made as to whether the record has historical value and merit permanent preservation. For the MOD this task is undertaken by DG Info-Corporate Memory Records (Info-CMemR), who assess the recommendations made by the originating business unit.

## 1.6 The Importance of Records to MOD

The MOD and the Armed Services are large and complex organisations whose decisions and actions affect many people, potentially over long periods. The various Business Units of MOD have a need to record decisions and actions for their own and wider MOD use. These decisions and actions are however increasingly open to legal, Parliamentary, media and personal challenge, often many years after the event. Business Units, whether it is the originator of the action or a successor branch, need to know what happened and why it is important. Selection of records for medium and long term preservation for administrative use needs care, foresight and experience; the judgements made at this stage must also be tempered with the need for the permanent preservation of some records, for the national record in TNA. If Business Units are in doubt over which of their existing records need to be kept for medium and long term use, advice and help should be sought from Info-CMemR.

Service Historical Branches also have a wide experience of the use of records by MOD Ministers, Business Units, the Services and also of the interests of historians, the media and the public in these records subsequent to their opening after 30 years. If in doubt, err on the side of caution and forward the material to Info-CMemR with a recommendation that it is considered for permanent preservation. Further guidance and information can be found in the Corporate Memory Guidance Leaflet 'Your Records are your Defence'.

# Chapter 2

## Role and Responsibilities

### 2.1 Responsibilities of the MOD Departmental Records Officer

All Government Departments are required to appoint a Departmental Records Officer (DRO) who is responsible for ensuring that information, both operational and administrative, is recorded and properly maintained so as to ensure that Departmental business is effectively and in line with the statutory requirements of the Public Records Acts, FOI Act, and other relevant legislation. The MOD DRO is part of DG Info and is Director Information Exploitation (D Info Exp) on whose behalf day to day responsibility is discharged by Info-CMemR AD.

The DRO is responsible for MOD's records storage facilities at TNT at Swadlincote and Central London, for the central review and assessment of records to determine whether they merit permanent preservation and for the Information Hub (iHub) or registry advisory service. The DRO is also responsible for the production of this JSP which details the minimum standards to be adhered to by all MOD business units and also identifies good records management practice.

### 2.2 The Role of the Directorate / Agency Records Officer

The maintenance of an effective system of record keeping requires a systematic approach. Administrative personnel and desk officers all have a part to play but it is important that the task is co-ordinated at management level. Each Directorate or Agency is responsible for the maintenance of the records it generates or receives; it is imperative that these records are managed efficiently and maintained in a way which allows ready access to those which are needed, while those records which are no longer of value are dispensed with in accordance with this JSP.

The Directorate or Agency Senior Information Officer [1](SIO) owns the information within the organisation, sets policy and culture and is accountable for the quality and provenance of the information produced and as such should appoint a Directorate Records Officer (DIRO) / Agency Records Officer (ARO) to ensure that effective records management procedures are put in place and maintained. The DIRO / ARO will also be responsible for co-ordinating the activities of subordinate Branch Records Officers and will be the prime point of contact with Info-CMemR. In appointing the DIRO/ARO Directors and Chief Executives must ensure that the appointee has sufficient authority within the organisation to co-ordinate the activities of Branch Records Officers; for this reason appointees should normally be at Band C1 (or Service equivalent) level. Directors / Chief Executive's should ensure that full contact details for the DIRO / ARO are forwarded to Info-CMemR and that these are updated to reflect any subsequent change.

The duties of the DIRO / ARO are:

[1] See the IM Handbook for more details.

- To appoint a Branch Records Officers (BRO) of the appropriate grade (normally Band C2 / Service equivalent) and ensuring that they are familiar with their role and responsibilities. Newly appointed BROs must be briefed on their role and responsibilities in line with the duties outlined in this JSP.
- To ensure that all Branch File lists have been approved by Info-CMemR and copies have subsequently been submitted to Info-CMemR for retention, each File List is to be accompanied by a Branch Disposal Schedule. (Note: This is not required within Service formations)
- To ensure that local records management instructions exist to augment those contained in JSP 441; these instructions should be reviewed to ensure that they are consistent with JSP 441 and are to be issued throughout the organisation. Suitable monitoring arrangements should be in place to ensure that records management procedures are embedded and maintained. If the DIRO /ARO determine that there is major weakness in the existing records management procedures within the branch it may be appropriate to recommend that a suitable change objective be incorporated into the Management Plan.
- To coordinate the efficient and timely review of registered files (and material held other than on such files) is being undertaken in line with the instruction issued in this JSP.
- To maintain an up to date list of all BROs in their area and full contact details must be forwarded to Info-CMemR.
- To ensure that BROs have suitable procedures in place to ensure that all new administrative personnel received any required records management training.

### 2.3 The Role of the Branch Records Officer

The Information Manager (IM) works to the SIO and sets in place the processes necessary to deliver the information requirements of the organisation. The IM manages the information flow and enforces information management activities on behalf of the SIO and therefore should be nominated as the Branch Records Officer (BRO). The BRO is responsible to the DIRO /ARO for the following functions:

- The creation and continuous maintenance of the Branch File List and subsequent Disposal Schedule, which identifies, where possible, the appropriate retention period and method of disposal of branch records - e.g. either destruction or archiving; ensuring that this information is submitted to Info-CMemR. The BRO will also be the focal point for liaison with Info-CMemR.
- The BRO may be given responsibility for the completion of all Registered File Disposal Forms (MOD Form 262F), consulting the relevant desk officer as necessary. Alternatively, this task may be carried out by desk officers.
- The maintenance of a definitive record of material held by the branch which is not located on registered files.

- Ensuring that comprehensive local instructions exist covering the working practices in the registry and that new members of staff receive suitable training upon arrival.
- The BRO should be the Line manager of the iHub or administrative personnel who maintain the Records on a day-to-day basis.
- The supervisor of the administrative personnel may be a Band D whose work may include much of the routine work involved with the Records, however, the BRO retains responsibility for ensuring that the procedures outlined in this manual and any subsequent local instructions are adhered to.

### 2.4 The Role of the iHub / Administrative Personnel Supervisor

The Information Support Officer (ISO) undertakes those administrative tasks necessary to support the collective use of information. The ISO would normally run an iHub or registry and hence has day-to-day responsibility for the following:

- The ongoing maintenance of the branch File List including the allocation of new file titles and numbers as required.
- The maintenance of the registered files and other records held by the branch in accordance with the instructions in this JSP, JSP 440 and local instruction.
- The closure of registered files in line with this JSP.
- The preparation of branch records for disposal in line with the branch Disposal Schedule.
- The maintenance of a system to record the whereabouts of registered files which have been removed temporarily from their permanent location within the Branch.
- The supervision of administrative personnel.

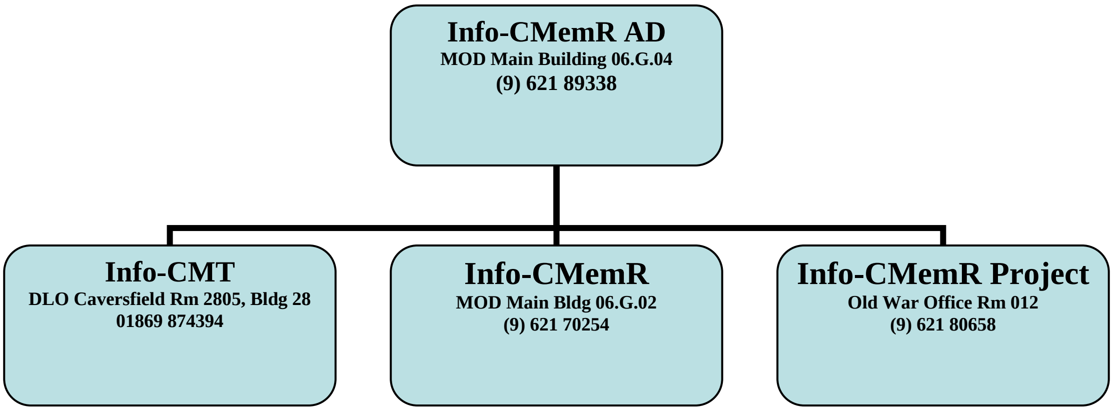
### 2.5 The Role of Desk Officers and Other Business Unit Personnel

Desk officers and other business unit personnel raising or receiving official correspondence have a responsibility to ensure that it is placed in the appropriate registered file. If the nature of the material makes it impossible to place in a registered file (for example, bulky material) then the nature and whereabouts of the material should be recorded.

Desk officers also have a responsibility to liaise with the BRO when they request the creation of a new registered file (or any other type of record) to ensure that a suitable entry is made in the branch Disposal Schedule. Subsequently, desk officers are likely to be involved in the completion of the Registered File Disposal Form (MOD Form 262F) which will ultimately confirm or amend the recommendation made in the branch Disposal Schedule.

## 2.6 The Organisation of DG Info-Corporate Memory Records

The Corporate Memory Records branch is sub-divided into paper records (Info-CMemR) and electronic records (Info-CMemERM) sections. Each section is led by an Assistant Director. The following diagrams display the structure of the records teams, followed by the key responsibilities of each part of the branch.



## 2.7 Role of Info-CMT (Contract Management Team)

Info-CMT (or Hd CMT as the post is often referred to) is responsible for the management of the MOD archives at Swadlincote in Derbyshire. The archives house most of the records in registered files along with unregistered records and a large quantity of Service personnel records and scientific and technical material. The Service personnel records are kept for an extended period, with the Lord Chancellor's authority, as reference may need to be made to them for many years after discharge, for instance, for pension purposes. Civilian personnel records which, like Service records are retained for an extended period are also housed at the MOD archives in Swadlincote, Derbyshire.

## 2.8 Role of Info-CMemR

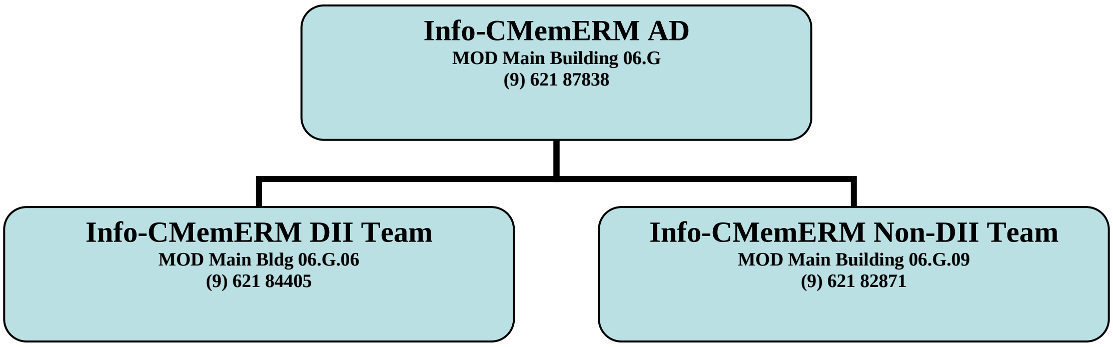
Info-CMemR is responsible for the review of records which are forwarded by business units to one of the two MOD archives. Records are generally reviewed no later than 25 years after their last record action. It is through this process, incorporating the recommendation made by the originating business unit, that records worthy of permanent preservation are selected. Records that are selected for permanent preservation are prepared by Info-CMemR for transfer to TNA.

Info-CMemR is responsible for the approval of the Main Headings and numbers for all MOD HQ (and other civilian business units) paper file lists, including the required Disposal Schedules. In addition, Info-CMemR responds to questions about the status of MOD records from other government departments, overseas governments and members of the public.

Info-CMemR is also responsible for the archive in central London which houses TOP SECRET and other sensitive material.

## 2.9 Role of the Info-CMemR Project

The Info-CMemR Project Team is responsible for the provision and scanning of the MOD Files that were previously contaminated with Asbestos in the Old War Office Building, London. The Project Team was established in autumn 2005 with a view to the project ending in late 2007, by which time contaminated files will have been processed into electronic medium.



Info-CMemERM AD
MOD Main Building 06.G
(9) 621 87838

Info-CMemERM DII Team
MOD Main Bldg 06.G.06
(9) 621 84405

Info-CMemERM Non-DII Team
MOD Main Building 06.G.09
(9) 621 82871

## 2.10 The Role of Info-CMemERM DII Team

The Info-CMemERM DII Team is responsible for setting corporate policy and practice for electronic records management on the DII. The team review and approve electronic file plans and associated retention schedules, identifying areas holding 'key' records which may warrant permanent preservation.

Info-CMemERM is developing corporate strategy for the long-term management and preservation of digital information, and is working closely with TNA to develop methods for the review and transfer of electronic records.

## 2.11 The Role of Info-CMemERM Non-DII Team

The Info-CMemERM Non-DII Team is responsible for the development of electronic records policy and practice for systems other than the DII, and directing its application across Defence. This will include developing techniques for the capture and preservation of records held on systems that do not have ERM capabilities.

# Chapter 3

## The MOD Paper Filing System

### 3.1 Registered Files

MOD, in common with other government departments, operates a filing system to account for the use of registered files. Each file relates to a particular subject, or aspect of a subject, and has a unique identifying reference (alpha/numeric combination). Purpose-designed file covers must be used and are to be ordered from Llangennech:

- **TOP SECRET** (Red) - MOD Form 329A;
- **SECRET** (Pink) - MOD Form 329B;
- **CONFIDENTIAL** (Green) - MOD Form 329C;
- **RESTRICTED/Unclassified** (Brown) - MOD Form329D.

Specific File Covers also exist for Atomic Records:

- Atomic File Cover TOP SECRET – MOD Form 0057A
- Atomic File Cover SECRET – MOD Form 0057B
- Atomic File Cover CONFIDENTIAL – MOD Form 0057C

### 3.2 Contents of a Registered File

All papers of substance must be placed on a registered file. Ephemeral papers, rough drafts, spare copies etc need not be placed on registered files if they are likely to be needed only temporarily and are not of any lasting significance. Such papers should be destroyed when no longer needed. If it transpires that such a paper has taken on a greater significance, it should be filed on the appropriate registered file.

### 3.3 The File List

[Note: The paragraphs below outline the requirements within MOD Headquarters and other non-Service areas. Service formations and units may, at their discretion, maintain a file list based on historical precedent though they may choose to adopt the one outlined here.]

The guidance which follows relates to the creation of a new file list. While this is not relevant to most business units, branches involved in reorganisations or mergers may need to do so. The underlying principles should also be applied when file lists are being amended or updated.

Within MOD Headquarters and other civilian business units the hierarchical structure is used. Such a system incorporates the use of "Main Headings" to identify the key activities of each business unit, with the use of subsidiary "Secondary Headings" and "Tertiary Headings" to identify more specific, subordinate, subjects.

### 3.4 The File List - Main Headings

In creating a hierarchical file list, the first task is to identify the Main Headings which will be required. It is impossible to be prescriptive about the main headings to be used, as they will be determined by the purpose and activity of each business unit. It is usual that the first main heading on a file lists is "Administration"; the other main headings should then be listed in order of significance and be dependant on the Organisation or Establishments key business.

### 3.5 The File List - Secondary (or Subsidiary) Headings

Having identified the main headings and listed them in order of importance, apply the same approach to the creation of subsidiary headings beneath each main heading. Ensure that activities which are linked appear together; e.g. after selection the main heading of “Administration”, the secondary headings might be subject like e.g. Personnel, Security, Organisation and Training.

### 3.6 The File List - Tertiary Headings

Having identified the main and secondary headings the same approach is now used to create the tertiary headings; e.g. “administration – Security –” followed by possible tertiary heading of inspections, breaches, or spot checks. When quoting the file titles, it is essential that the headings are separated with a dash (–) to avoid confusion. By applying the same principle throughout the file list, a logical and straightforward file index will be created which is consistent and easy to follow.

### 3.7 General Principles of File Headings

File titles, which must have a minimum of two headings, should not normally exceed three headings e.g. main, secondary, and tertiary; where absolutely necessary the use of additional sub-headings is permissible.

Terms such as "General", "Miscellaneous" and "Policy" are too vague to be appropriate for use as main headings and must be avoided for use as secondary or tertiary headings wherever possible. All headings should be specific and should clearly identify the nature of the material to be contained within the file.

Use of abbreviations and acronyms must be avoided. Where they are used the words represented must be included in full in the file title and the abbreviation / acronym inserted in brackets thereafter.

### 3.8 The File Reference

Each file must be allocated a unique file reference. This will be an alpha/numeric combination which serves to ensure that the file which has been created is not confused with any other file. Each element of the reference should be separated by an oblique stroke (**/**) to distinguish each individual component.

The first element of the alpha/numeric file reference is the business unit or Directorate short title. If the business unit short title ends with a number, the number must be bracketed to avoid confusion with the overall file reference.

The business unit title should be followed by the file reference number. The number of headings in the file title will dictate the amount of numbers required in the file reference number‘ e.g. a file entitled "Administration-Security" will have two numerical elements, while a file entitled "Administration-Security-Inspections" will have three. A practical example of file heading and references that could form a part of the Info-CMemR File list would appear as:

| File Reference Number | Main Heading | Secondary Heading | Tertiary Heading |
|---|---|---|---|
| DG Info-CMemR/1/1/1 | Administration - | Security - | Inspections |
| DG Info-CMemR/1/1/2 | Administration - | Security - | Breaches |
| DG Info-CMemR/1/1/3 | Administration - | Security - | Spot Checks |
| DG Info-CMemR/2/1/1 | Records Management - | Disposal Schedules - | TNA Guidance |

In the event of a gap in the numbering the unused number should appear on the file list but carry the annotation "**RESERVED**".

### 3.9 Approval of the File Structure, Main Headings and Reference Numbers

The file structure, main headings and numbers of all MOD HQ and other business unit file lists must be approved by Info-CMemR before use. Once approval has been granted the new file list should be constructed with the following information:

- Secondary and tertiary headings and full reference numbers should be allocated.
- A copy of the full file list, incorporating a Disposal Schedule, is to be forwarded to Info-CMemR within 3 months of its introduction.
- Any proposed changes to main headings or numbers must also be approved by Info-CMemR prior to their incorporation into the file list.
- An up to date copy of the file list is to be forwarded annually to Info-CMemR.

### 3.10 General Principles of Creating or Updating a File List

When creating a new or updating an existing file list, be aware that if the Directorate or business unit short title is unchanged from the previous file list, then the main heading numbers cannot be used again. In such circumstances the new main headings must be allocated numbers which do not clash with the previous system. This is to avoid confusion resulting from the same file reference being used, but with different short titles.

Service formations and units have, historically, used different methods of referencing registered files and are not required to obtain approval from Info-CMemR before creating or amending file lists. If these Service formations wish to adopt the MOD HQ filing system they should contact Info-CMemR for the necessary advice.

### 3.11 Maintenance of an Approved File List

The BRO must maintain a definitive copy of the file list which should be amended when new files are created; changes are made to the disposal recommendation or change of “owner” of the file. The BRO has ultimate responsibility for the maintenance of the list though day-to-day responsibility may be delegated to the iHub or administrative supervisor.

The completed file list must incorporate a disposal schedule recommendation for all files and also the “owner” of the file, usually the post title of the relevant desk officer. The “owner” is responsible for identifying the disposal recommendation and the eventual completion of the Registered File Disposal Form (MOD Form 262F). More information on creating and maintaining a Disposal Schedule is contained in Chapter 4.

### 3.12 Opening a Registered File

When initially creating the registered file cover (MOD Form 329A, 329B, 329C or 329D) the following must be taken into consideration:

- The full file title, as it appears in the file list and designated file reference MUST be entered on the front cover of the file.
- The opening date of the file (date of origin of the first enclosure) MUST be recorded; no file should be opened until there is an enclosure to be placed in it.
- The file should be annotated with a part number, in the case of a new file this will be part A; additional parts number will be B, C, D etc. If Part Z has been reached the subsequent part number will be "Part AA" followed by "Part AB" and so on. The part number should NOT be included when recording the file reference on correspondence.

### 3.13 The Registered File Record Sheet (MOD Form 262A)

When a new registered file is opened its existence must be recorded on a Registered File Record Sheet (MOD Form 262A). When a registered file is closed the date of closure is to be recorded on the MOD Form 262A in the designated area.

The Registered File Record Sheet is the definitive record of a file's existence. If subsequent parts to the file are opened then a new MOD Form 262A is to be raised for each part. They are to be placed in binders (MOD Form 262) and maintained until replaced by a Registered File Disposal Form (MOD Form 262F).

If a registered file is sent temporarily to another business unit the Registered File Record Sheet must be used to identify:

- The details of the Business unit to which it was sent;
- The date it was sent;

- The date it was received back into the business unit.

The Registered File Record Sheet may also be used to record that a file has been issued to a member of staff within the business unit. Alternatively, it may be more practical to maintain a separate system to record file movements within the business unit.

Whichever method is used, a system of identifying the whereabouts of files which are removed from the registry must be established, both to ensure effective file management and to satisfy security requirements.

### 3.14 Placing Documents onto Registered Files

It is important to ensure that material which is deemed worthy of retention on a registered file is placed on the file as soon as possible. The registered file is the definitive record of business unit activity on any given subject and it is imperative that anyone using a file can be confident that the information it contains is complete and up-to-date.

Documents should be placed on the right hand side of the file and secured by an India or bar tag to form enclosures within that file. Enclosures should be placed on the file in date of origin order (not date of receipt) and each enclosure should be sequentially numbered, e.g. **E1**, **E2** etc.

Late enclosures should also be filed in date of origin order. This will mean inserting them between existing closures. Existing enclosure numbers should not be deleted and changed. Instead, the new enclosure is to be given the number of the immediately preceding enclosure followed by a sub-number; e.g. If three late enclosures were to be inserted between the existing enclosures **E2** and **E3** they would be numbered **E2/1**, **E2/2** and **E2/3** respectively. The original **E2** would then be amended to reflect the number of additional enclosures which have been added in front of it, e.g. in this case **E2+3**.

In instances where an item is too bulky to place within the file details of the item (title; reference; date; physical location) should be entered on the file minute sheet. When the file is closed, the item is to be passed with the file to the “owner” for appropriate action.

The classification of the enclosures is to correspond to the classification of the Registered File Cover (as detailed in paragraph 3.1). For example a File may contain a majority of unclassified information and only one TOP SECRET document, however, the File will be classed as TOP SECRET. Should an unclassified File exist and a new document classified as “SECRET or above” need to be placed on it, the file is to be:

- Upgraded, the File cover is to be changed (paragraph 3.20)
- MOD Form 262A (File Record Sheet) is to be annotated (paragraph 3.13)
- MOD Form 672 (Record of Classified Document (TOP SECRET and SECRET)) is to be placed in the file (paragraph 3.18)
- The document is to be recorded in MOD Form 102 (Protected Document Register) (paragraph 3.18). Details on the completion and management of MOD 102 can be found in JSP 440, Part 5, Chapter 2.

### 3.15 The File Minute Sheet

The file minute sheet is a plain piece of A4 paper that is to be placed on the left-hand side of the file, a new minute should be listed on the sheet; each minute should be numbered and the classification of the minute should be indicated. It is used to record:

- Any significant comments about the content of the file
- Details of significant enclosures on the file
- Details of any contents which will require the retention of the file for a specified period for administrative purposes
- Details of any contents which appear to have historical value that will merit a recommendation for the file to be passed to Info-CMemR.

When a file is being passed to a colleague for action a covering minute can be placed on the minute sheet. When this is done the minute or enclosure number should be entered on the front cover of the file along with the title of the person to whom the file is being referred.

### 3.16 Transfer of Enclosures Between Registered Files

Enclosures must only be transferred between files if they have been misfiled.

When an enclosure has been misfiled and the action is to remove the item, the following information should be recorded either on the file minute sheet or on a piece of paper inserted in place of the enclosure:

- the date of removal of the enclosure
- the documents reference
- the protective marking
- the file number of the file to which it has been transferred
- the new enclosure number
- the signature of the officer authorising/making the transfer

When an enclosure that has been misfiled is to be inserted into a different file, the transferred enclosure should be inserted on the new file in date of origin order. The original enclosure number should be crossed out (but not deleted) and the document annotated with the relevant new enclosure number. A note should be added to the file minute sheet recording the following details:

- The document's previous file reference and enclosure number
- Any protective marking
- The date of transfer
- The signature of the officer authorising/making the transfer

### 3.17 Temporary Enclosure Jackets

Temporary Enclosure Jackets (TEJs) are to be used when there is a need to consult others about papers on a registered file but it is not convenient to forward the complete file. Copies of the relevant papers along with covering correspondence may be placed in a TEJ (MOD Form 174A (**TOP SECRET**), MOD Form 174B (**SECRET**), MOD Form 174C (**CONFIDENTIAL**) and MOD Form 174D (**RESTRICTED/Unclassified**)) of appropriate classification and forwarded to the appropriate business unit, bearing the following information:

- A separate Registered File Record Sheet (MOD Form 262A) should be raised to record the existence of the TEJ and to whom it has been sent.
- The TEJ should bear a protective marking appropriate to its own contents and not necessarily the marking borne by the parent file.
- A "Record of Classified Documents (TOP SECRET and SECRET)" (MOD Form 672)" must be included for material classified as SECRET and above.
- The TEJ should bear the file reference and title of the parent file with the addition of its own TEJ number, e.g. "TEJ NO 1" and so on.

The TEJ must be returned to the originating business unit for incorporation into the parent file as soon as possible, through the following means:

- it should be placed in the file in date order (according to the date returned which should be marked on the TEJ cover)
- It is to be allocated an enclosure number
- The file minute sheet should be annotated to record the enclosure number of the TEJ along with details of the number of enclosures contained within it.
- The TEJ Registered File Record Sheet (MOD Form 262A) should be annotated to record the date on which the TEJ was incorporated into the file.
- Once incorporated into the file no further enclosures are to be added to the TEJ.

### 3.18 Record of Classified Documents (TOP SECRET and SECRET)

In addition to the previously described requirements of a registered file there are additional requirements for Registered Files classified as "SECRET" and "TOP SECRET". Along with the file minute sheet a "Record of Classified Documents (TOP SECRET and SECRET)" (MOD Form 672) must be placed on the left hand side of the file.

When an enclosure classified as "SECRET" or "TOP SECRET" is placed on a file its existence and enclosure number must be recorded on the "Record of Classified Documents (TOP SECRET and SECRET)" (MOD Form 672) and also be entered into the Protected Document Register (MOD Form 102).

*The instruction for maintaining, sending and receiving classified material is contained within JSP 440 - The Defence Manual of Security. This guidance* *also included retention periods of the MOD Form 102 and the storage requirements for such material.*

### 3.19 Access to Registered Files

Registered files may be circulated to anyone within MOD on a "need to know" basis, provided they are cleared to the appropriate level. They may also be circulated to other government departments or external legal advisers and to the National Audit Office, where appropriate. Files are <u>NOT</u> to be sent to any other location without the prior approval of Info-CMemR.

Where necessary, and with the approval of the Head of Business Unit, a file may be marked *"Not to be sent outside the business unit without the approval of .... [a named individual]".*

### 3.20 Upgrading of Registered Files

It will sometimes be necessary to upgrade a file to reflect the fact that a new enclosure is of a higher classification than the existing file. When this is the case, a new file cover should be produced and given an identical number to the old cover.

The contents of the old file should be removed and transferred to the new cover along with the top half of the front of the old cover which should be placed in the new file on the left hand side.

The date of opening of the original file should be entered on the front cover of the upgraded file (e.g. not the date on which the file was upgraded). The date on which the file was upgraded should be entered beneath the date of opening. The File Record Sheet (MOD Form 262A) must also be amended to show the date of upgrading, along with the new protective marking.

If there is a subsequent need to upgrade the file again then the above action should be repeated. The top half of each pre-existing file cover should be retained in the new file.

Remember that if a file is upgraded to SECRET a "Record of Classified Documents (TOP SECRET and SECRET)" (MOD Form 672), will need to be raised and inserted in the file on the left-hand side (Paragraph 3.14).

File covers denoting a classification higher than the first enclosure(s) are not to be used in anticipation of material which might be placed on the file later.

### 3.21 Transfer of Files to Another Government Department or MOD Business Unit

If the need arises to transfer a file permanently to another government department, Info-CMemR must be consulted before any transfer action is taken.

The need may arise to transfer a single/or series of files to another MOD business unit. For example, when a reorganisation results in the transfer of responsibility for a particular project to a different business unit or an entire business unit being transferred to another directorate.

When such a need arises it may be possible to retain the existing file numbers and amend the business unit title on the file covers. Info-CMemR should be advised in writing if such action is taken.

In most circumstances, if parts of a file series are being permanently transferred to a new business unit the relevant files should be closed and forwarded to the "importing" business unit which will open appropriate files, allocate new file reference numbers, and raise new Registered File Record Sheets (MOD Form 262A).

It may however not be practical to retain the existing file number (e.g. in cases where the existing number duplicates a number already used by the "importing" business unit) in which case the existing files will need to be closed and new files opened by the "importing" business unit which can then allocate new file numbers.

In no circumstances may a file be renumbered. If there is a need to allocate a new number the file must be closed and a new file opened. The files should then be cross-referenced.

In all cases, the appropriate MOD Form 262As must accompany the transferred files to the "importing" business unit where they should be attached to the new MOD Form 262As. The "exporting" business unit must formally record the transfer of the files in the File List and may, additionally, retain a copy of the relevant MOD Form 262As annotated to record the transfer. The "exporting" business unit must also notify Info-CMemR of the transfer.

Where the exporting business unit retains previous (closed) parts of the file they should also be forwarded to the importing business unit. Additionally, any Registered File Disposal Forms (MOD Form 262Fs) held for previous parts of the file should be forwarded.

### 3.22 Missing Files

If, after a thorough search, a registered file cannot be located, a written report is to be submitted to Info-CMemR. The report is to identify the file concerned, its protective marking, and the nature of its contents and is to contain an explanation of the circumstances surrounding its loss. If the file contained classified information a report is also to be submitted to the appropriate security directorate in accordance with the instructions in JSP 440 - The Defence Manual of Security.

### 3.23 When to Close a Registered File

There are a number of factors which need to be assessed when determining whether to close a file. If any of the following criteria apply the file should be closed:

- The file is 1 inch thick;
- The file contains 100 enclosures;
- The file has been open for 5 years;
- Nothing has been added to the file for the last year (close the file unless there is a clear indication that papers will be added to it shortly);
- Action on the subject covered by the file has come to an end.

### 3.24 Closing a Registered File

The following actions are to be taken when closing a registered file:

- Mark the file boldly on the front cover "CLOSED - NO NEW PAPERS TO BE PLACED ON THIS FILE".
- Note the date of closure on the MOD Form 262A along with the date of the last enclosure on the file.
- Raise a Registered File Disposal Form (MOD Form 262F). The file title, file reference, part number, and protective marking (where applicable) should be entered on the form along with the date of the last enclosure and the date of closure of the file. Section 1 of the form should then be completed. This records the Disposal Schedule recommendation.
- Check the file minute sheet to see whether the file contents include any items which, because of their bulk, could not be placed within the file; If so then ensure that these items are passed with the file to the relevant "owner" for review.
- Insert the MOD Form 262F, completed as above, onto the file on the right hand side, (e.g. on top of the last enclosure).
- Pass the file to the "owner" to review and completion of sections 2 and 3 of the MOD Form 262F.
- When the file is returned by the "owner", action should be taken in accordance with the instructions on the MOD Form 262F. If the file is to be retained locally prior to destruction or passage to Info-CMemR a B/F (bring/forward) date should be recorded and the file stored with the other closed records held by the business unit.
- Closed files should be kept separately from open files.

**NOTE:** Guidance for completing MOD Form 262F can be found at ANNEX A to Chapter 3.

### 3.25 "Weeding" of Registered Files

Heads of Business Unit should NOT authorise the weeding of registered files**.** One of the reasons for this is that the process of weeding files is a time-consuming and therefore a costly activity. A second reason is that TNA requires MOD to select complete files for permanent preservation rather than extracts from files. This is to ensure that preserved documents retain their original context.

### 3.26 Miscellaneous material NOT placed on Registered Files

Not all records will be placed in registered files. Records may be in a range of other forms such as maps, plans, drawings, charts, video, film, photographs, Technical Reports etc. Additional guidance is given in Chapter 7.

# Chapter 3 - Annex A

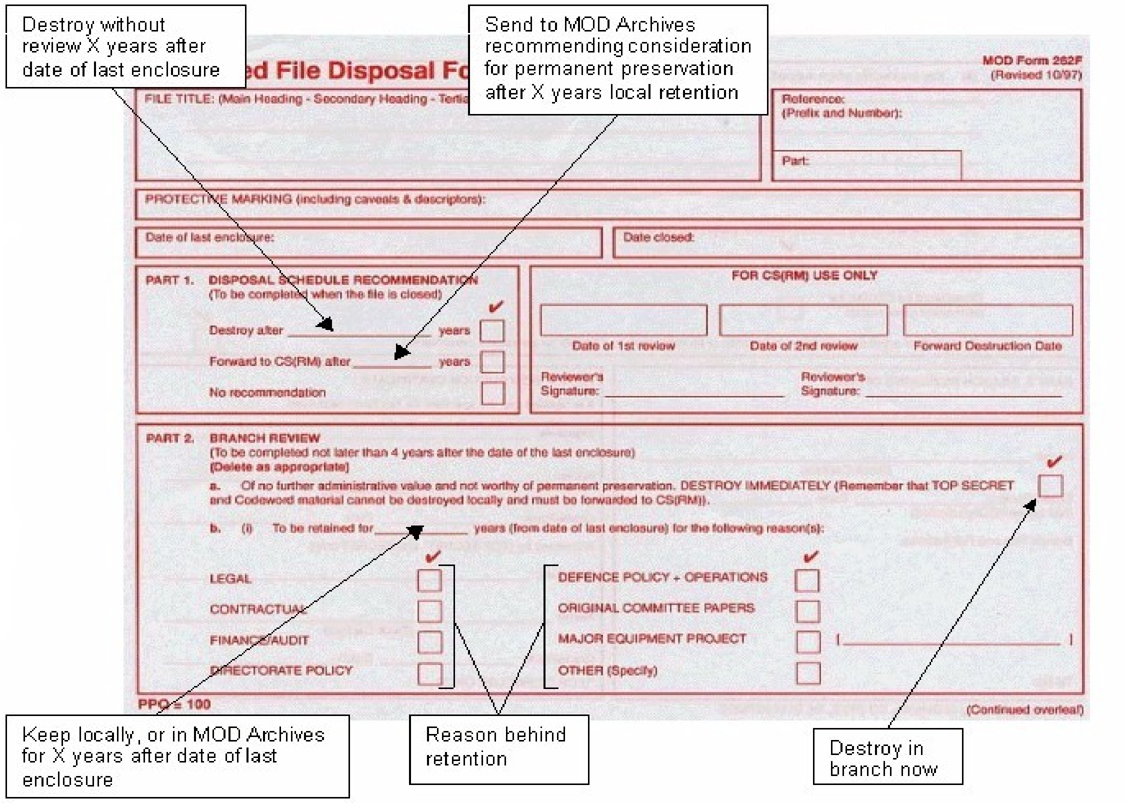
## Completing the Registered File Disposal Form

1. **When should a registered file be closed?**
   - The file is 1 inch thick.
   - The file contains 100 enclosures.
   - The file has been open for 5 years.
   - Nothing has been added to the file for the last year (close the file unless there is a clear indication that further enclosures will be added to it shortly).
   - Action on the subject covered by the file has come to an end.
2. **Actions to be taken by Administrative Personnel**
   - The front cover of the file should be boldly annotated "CLOSED - NO NEW PAPERS TO BE PLACED ON THIS FILE".
   - A Registered File Disposal Form (MOD Form 262F) should be raised .The full file title, full file reference (prefix and number), part number, and protective marking should be entered on the form along with the date of the last enclosure and the date of closure of the file. Part 1 of the form should then be completed. This records the Disposal Schedule recommendation.
   - Insert the MOD Form 262F, completed as above, onto the file on the right hand side, (i.e. on top of the last enclosure).
   - Pass the file to the appropriate desk officer for review.
3. **Actions to be taken by the Desk Officer / Reviewing Officer**
   - Consult Part 1 of MOD Form 262F to determine whether a disposal schedule recommendation has been recorded.
   - Taking account of the disposal schedule recommendation, complete Part 2 of the form identifying:
     - the appropriate retention period for the file;
     - any key enclosures which support the recommendation;
     - whether at the end of any retention period specified for administrative use, the file merits consideration by Info-CMeMR for permanent preservation.
   - Complete and sign Part 3 of the form and return it to the registry.
4. **After completion of the MOD Form 262F**
   - Noting the decision made by the Reviewing Officer record the relevant B/F action for the file and place on the file, in the correct numerical order, with the other closed records held by the branch. (Note that closed files should not be stored alongside open files.)

- When a file is destroyed by the branch the MOD Form 262F is to be removed and used to replace the Registered File Record Sheet (MOD Form 262A) which should then be destroyed.
- If the file is not destroyed locally but is forwarded to the relevant archive the original MOD Form 262F must accompany the file. The branch should retain a copy of the MOD Form 262F, annotate it to indicate that the file has been forwarded to Info-CMemR and use it to replace the MOD Form 262A, which should be destroyed.
- The Registered File Record Sheet (MOD Form 262A) and Registered File Disposal Form (MOD Form 262F) are the definitive record of a file's existence and subsequent destruction/passage to Info-CMemR. MOD Form 262A must not be destroyed until replaced by MOD Form 262F. Each MOD Form 262F must be retained for a period of at least 30 years from the date it replaces the MOD Form 262A. As MOD Form 262Fs are normally retained in a binder relating to a file series or a number of file series, the binders should normally be retained for a period of at least 30 years following the insertion of the final MOD Form 262F. If a business unit is disbanded during this period the forms should pass to the successor business unit. If there is no successor business unit the binders should be forwarded to Info-CMemR.
- When files are to be forwarded to the relevant archive care should be taken when completing Section 2 of the form. Ensure that the recommendation about the file's disposal is sufficiently detailed and identifies clearly why the file is being recommended for further retention.

## 5. **A practical example**

See the attached sample MOD Form 262F with some useful tips on completing the form correctly.



Destroy without review X years after date of last enclosure

Send to MOD Archives recommending consideration for permanent preservation after X years local retention

...ed File Disposal Fo...

MOD Form 262F
(Revised 10/97)

FILE TITLE: (Main Heading - Secondary Heading - Terti...

Reference:
(Prefix and Number):

Part:

PROTECTIVE MARKING (including caveats & descriptors):

Date of last enclosure:

Date closed:

PART 1. DISPOSAL SCHEDULE RECOMMENDATION
(To be completed when the file is closed)

✓

Destroy after ____________ years □

Forward to CS(RM) after ____________ years □

No recommendation □

FOR CS(RM) USE ONLY

| | | |
|---|---|---|
| Date of 1st review | Date of 2nd review | Forward Destruction Date |

Reviewer's Signature: ____________

Reviewer's Signature: ____________

PART 2. BRANCH REVIEW
(To be completed not later than 4 years after the date of the last enclosure)
(Delete as appropriate)

✓

a. Of no further administrative value and not worthy of permanent preservation. DESTROY IMMEDIATELY (Remember that TOP SECRET and Codeword material cannot be destroyed locally and must be forwarded to CS(RM)). □

b. (i) To be retained for ____________ years (from date of last enclosure) for the following reason(s):

| ✓ | | ✓ |
|---|---|---|
| LEGAL □ | DEFENCE POLICY + OPERATIONS | □ |
| CONTRACTUAL □ | ORIGINAL COMMITTEE PAPERS | □ |
| FINANCE/AUDIT □ | MAJOR EQUIPMENT PROJECT | □ [____________] |
| DIRECTORATE POLICY □ | OTHER (Specify) | □ |

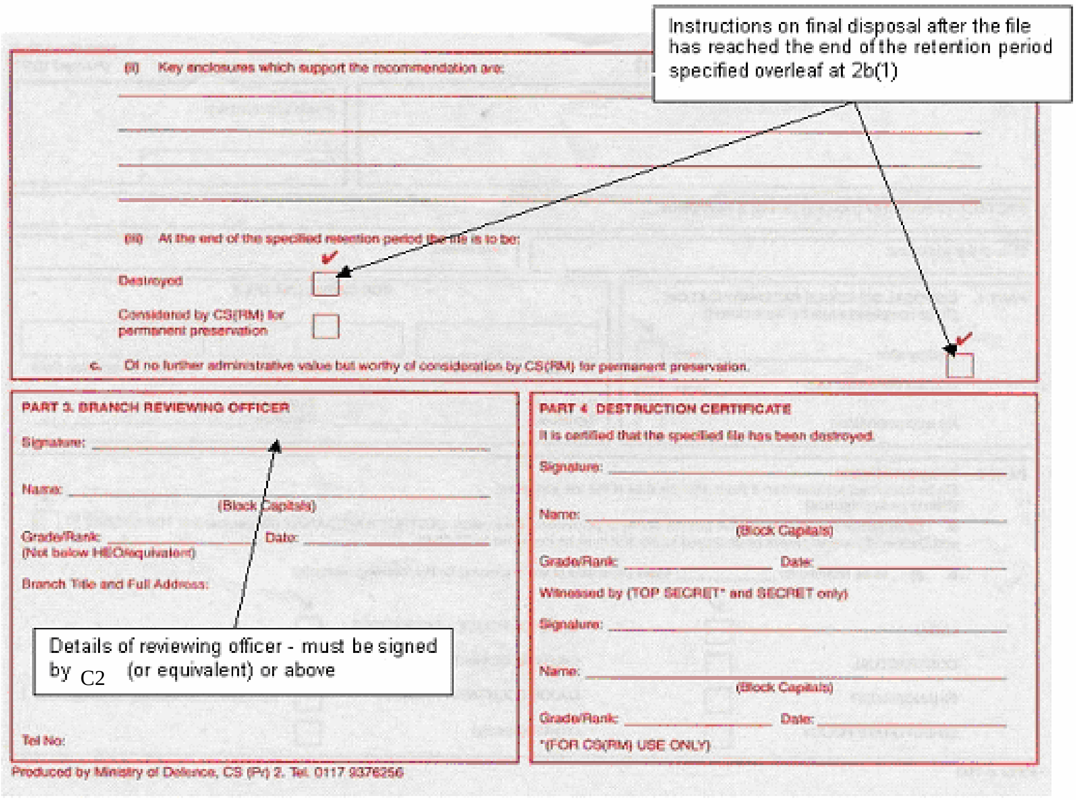
PPQ = 100

(Continued overleaf)

Keep locally, or in MOD Archives for X years after date of last enclosure

Reason behind retention

Destroy in branch now



Instructions on final disposal after the file has reached the end of the retention period specified overleaf at 2b(1)

(ii) Key enclosures which support the recommendation are:

____________

____________

____________

____________

(iii) At the end of the specified retention period the file is to be:

✓

Destroyed □

Considered by CS(RM) for permanent preservation □

c. Of no further administrative value but worthy of consideration by CS(RM) for permanent preservation. ✓ □

PART 3. BRANCH REVIEWING OFFICER

Signature: ____________

Name: ____________
(Block Capitals)

Grade/Rank: ____________ Date: ____________
(Not below HEO/equivalent)

Branch Title and Full Address:

Tel No:

Details of reviewing officer - must be signed by C2 (or equivalent) or above

PART 4 DESTRUCTION CERTIFICATE

It is certified that the specified file has been destroyed.

Signature: ____________

Name: ____________
(Block Capitals)

Grade/Rank: ____________ Date: ____________

Witnessed by (TOP SECRET* and SECRET only)

Signature: ____________

Name: ____________
(Block Capitals)

Grade/Rank: ____________ Date: ____________

*(FOR CS(RM) USE ONLY)

Produced by Ministry of Defence, CS (Pr) 2. Tel. 0117 9376256

# Chapter 4

## Review of Records Held by Business Units

### 4.1 The Lifecycle of the Registered File

Within MOD the DRO has delegated the authority to HQ business and service units to review their own records. In a majority of cases this will mean destroying the records locally that are not considered worthy of permanent preservation or cease to have an administrative value. The exception is that all registered files containing TOP SECRET and Codeword material are to be forwarded to Info-CMemR and are NOT to be destroyed locally.

All registered files that are identified by the business unit as meriting consideration for permanent preservation are to be sent to the relevant archive. Certain Air Force department files may initially be sent to the Air Historical Branch (RAF) with the prior agreement of both the Air Historical Branch and Info-CMemR.

Info-CMemR conducts a review of registered files 25 years after the closure of the file. The review allows a judgement to be made about the historical context of the records. Files which are selected for permanent preservation are normally passed to TNA and are then made available to the public in line with the terms of the Public Records Act of 1958 and1967.

Annex A to Chapter 4 has been created to offer guidance and an overview of good records management practices.

### 4.2 Review of Material by the Business Unit

Business units are to ensure that an effective system of review is maintained through a disposal schedule, allowing those records which are no longer needed, and do not merit permanent preservation, to be destroyed, while records which are needed for administrative purposes are kept for the appropriate period and those which appear to merit permanent preservation are forwarded to the relevant archive.

In reviewing the records which they hold, each business unit should consider the appropriate length of time that a file, or any other type of record, is likely to be needed for administrative purposes; additionally an initial judgement can be made about the likely historical value of a file.

When reviewing classified material which is to be retained for administrative or historical reasons, consideration should be given as to whether the material continues to merit its original protective marking, or whether it should be downgraded.

### 4.3 Creating the Disposal Schedule

The Disposal Schedule will help each business unit to identify, where possible, an appropriate length of time for which each Registered File/Record should be kept and how it should ultimately be disposed of. Disposal may be to the relevant archive with a recommendation that the file warrants permanent preservation, or it may be through local destruction. As most records held should be on registered files the Branch File List should be the basis of the Disposal Schedule.

The Branch Records Officer is responsible for drawing up the Disposal Schedule. However, the task of recommending suitable retention periods for each file is best performed by the desk officers who use the files. They should be best placed to make this judgement based on their working knowledge of the nature of the file and its content. The Branch Records Officer's role is to co-ordinate this task.

Each file will contain records which fall into one of the following categories:

- Records which merit consideration by Info-CMemR for permanent preservation;
- Records which will need to be kept for an extended period for administrative purposes (perhaps for legal or contractual purposes);
- Records which have only short term value and will only need to be retained for a specific period of time.

Establishing a Disposal Schedule involves considering all of the existing files held by the business unit and identifying, the category each file (or group of files) falls into. The different types of information held within any particular business unit might include:

**Administrative Records** - These records are produced in large volumes, generally they have low retention values and may be disposed of within 1 to 7 years after the date of creation.

**Case Records** – The retention periods for these records are usually defined by an individual's age and life span unless a statutory or a long-term operational requirement defines a period for their continued retention. For example, records relating to criminal investigations or Boards of Inquiries may be retained, depending on the subject for 75 years or more.

**Command and Control and Operational Records -** Some records in these categories can have a long life span and should, in many cases, be considered for permanent preservation.

**Estates and Accommodation Records -** These records include a substantial amount of administrative type records with a low retention value, however certain records may be retained for much longer periods e.g.

- Legal records – estate title, leasehold documentation, etc., should be retained for at least the occupancy period.

- Policy records – surveys, policy studies etc., retention varies between 10 to 25 years but there may be records relating to important aspects such as disposal of potentially hazardous substances on sites or other health and safety issues that should be kept for much longer periods of time.

**Finance Records** - These records normally have a short working life of about two years. Generally there is no legal requirement to retain these records beyond seven years.

**Health and Safety Records** – As well as some statutory requirements that need to be complied with, there are those records that can have a very long retention requirement; a retention period of up to 100 years may be required in these cases.

(NOTE: JSP 375 - The MOD Health & Safety Handbook also offers guidance).

**Personnel Records** - The retention periods for these records may vary but some should be kept for very long periods. Examples include:

- Pension - Documents that have a bearing on pension entitlement should be kept for up to 100 years from date of birth.
- Military Personnel - Service personnel appraisal reports are to be kept for 100 years from date of birth.
- Civilian Personnel - Civilian Staff appraisal records are normally kept for up to 100 year from date of birth as separate sub-sets of personal files. If kept in annual sets, they should be destroyed on a rolling basis.
- Medical - Medical records are normally filed as a separate sub-set of individual personal files to allow for separate retention. In some instances where they relate to, for example, exposure to radiation, these may be kept for up to 100 years.

**Policy Records** - These are normally retained for at least 25 years, and in cases where the records relate to the development of primary legislation, may be marked for permanent preservation.

**Scientific, Technical and Research Records** – Records of the more important aspects of scientific, technological or medical research and development are normally retained as a long term research resource for other scientific researchers. Retention periods may differ, as some business units may retain these records as part of their permanent library, whilst others may consider them as case files and dispense with them after 10 years. Reports for these types of records are normally preserved, whilst the supporting information is not, however their administrative value could be long, i.e. Porton Down and paper records covering the volunteer programme go back to the 1950's.

**Transaction Records** - these records record specific events that have a finite life, i.e. the award of a contract allocated to a named contractor to commission a particular task. Depending on the nature of the transaction, the retention period may vary between 6 to 25 years.

The varying management requirements for each of the types of information listed above also need to be considered. Factors to be considered include:

- Operational requirements.
- Business requirements.
- MOD corporate requirements.
- Public access requirements.
- Legal and statutory requirements.
- Human life expectancy.
- Volume of records likely to be generated.

The recommendations made should then be noted in the Disposal Schedule. In addition to the file list the "Record of Unregistered Material" should also be considered and appropriate recommendations made, where possible. An example of an extract of a completed Disposal Schedule is at Annex B. Further guidance about how long to keep Records can be found at Annex C.

The records officer/desk officer who ultimately completes the Registered File Disposal Form (MOD Form 262F) may not agree with the recommendation and is free to change it. This might be necessary if subsequent events have given a different weight to the content of the file. However, where this is not the case, the recommendation can be endorsed with the confidence that it was the considered opinion of a predecessor who was familiar with the nature of the contents of the file.

Where it is not possible to make a recommendation about the disposal of a file the words "No Recommendation" should be entered on the Disposal Schedule.

### 4.4 Examples of Records likely to warrant Permanent Preservation

Documents/Files

- Containing TOP SECRET or Codeword material.
- Containing information on important scientific/technical developments.
- Used by Official Historians or have been marked for retention by them.
- That illustrates the formation/evolution of Defence Policy or significant developments in the relationship between MOD and other organs of Government, or other national or international authorities.
- That shows the authority under which MOD has exercised a function.
- That contain important decisions relating to the organisation, disposition or use of the Armed Forces
- That shows the reasons for important decisions, actions or provides precedents. That could help the Government to establish, maintain, or control a legal claim or a title that reflect Law Officers opinion on any subject.

Documents/Files and other records

- Of the setting up, proceedings and reports of committees, working parties and study groups.

- Of the introduction/consideration of new types of weapons and equipment.
- Of important trials and exercises.
- Of the introduction of new types of uniforms, clothing etc
- Of the formation, organisation, reorganisation, re-designation or disbandment of units.
- Of notable legal matters.
- Of the occupation of historic buildings and sites of archaeological interest.
- Of matters of significant regional or local interest which are unlikely to be documented elsewhere.
- Of subjects of general national or international interest.

Reports

- Of significant operations, intelligence, organisational and logistic matters.

Histories

- Produced by Service units etc.

Standing Orders

- Similar instructions of Commands, Agencies, Establishments etc.

Diaries

- Journals, logs etc providing an insight into particular operations or activities of wide interest

Records

- Relating to famous or infamous people.

**Note:** In assessing whether a file merits passage to Info-CMemR with a recommendation that it be considered for permanent preservation it is important to remember that it is the responsibility of the lead business unit to identify and forward such files. If your file merely contains copies of correspondence relating to a topic for which another business unit has lead responsibility the file need not be forwarded to Info-CMemR.

### 4.5 Maintaining the Disposal Schedule

The records officer is responsible for the maintenance of an up to date Disposal Schedule and the incorporation of amendments. The records officer is also responsible for ensuring that all desk officers have access to a copy of the schedule.

In many cases the recommendation will remain valid even when the existing file is closed and a new part opened. For instance, if a file has been recommended for passage to Info-CMemR because it illustrates significant developments in an area of policy, it is quite likely that any subsequent part of that file will fall into the same category. It may be that subsequent parts of a file increase or diminish in importance in relation to previous parts. Where this is the case the desk officer should advise the records officer to amend the Disposal Schedule accordingly.

As new files (as opposed to new parts of existing files) are opened the records officer should establish whether an initial recommendation about disposal can be made.

### 4.6 Timing of Review and Use of the Disposal Schedule

When a file is closed a Registered File Disposal Form (MOD Form 262F) is to be raised and placed in the file; at that time the Disposal Schedule is to be consulted to determine what recommendation has been made about the appropriate retention period and method of disposal. The disposal schedule recommendation should be noted on the MOD Form 262F and the file should then be passed to the desk officer responsible for reviewing the file and completion of the MOD Form 262F. The desk officer responsible for carrying out the review must then consider the recommendation and either endorse or amend it.

The MOD Form 262F should be completed and signed by an officer of at least Band C2 (or equivalent) grade (where necessary the desk officer must arrange for the form to be signed by the records officer or a line manager). If the ultimate recommendation is that the file should be retained for an extended period for administrative purposes, or that the file warrants permanent preservation, the specific enclosures which justify that recommendation (which should be identified on the file minute sheet) should be recorded on the MOD Form 262F. If there are a large number of enclosures which justify such a recommendation only the key enclosures need be identified.

Unregistered records are to be reviewed within 4 years of their creation to determine the appropriate method of disposal. Any such records which merit consideration by Info-CMemR for permanent preservation should be forwarded in accordance with the instructions at Chapter 7.

### 4.7 Existing Files Not Reviewed at Time of Closure

It is recommended that all files are reviewed at the earliest opportunity, and sections 2 and 3 of MOD Form 262F on completion of this review. Business units holding registered files (or unregistered records) which have not been reviewed must take remedial action to deal with the review backlog. MOD Form 262F should be raised and the files should then be reviewed and disposed of accordingly.

### 4.8 Retention of Registered Files by the Business Unit

If the completed and signed MOD Form 262F recommends that the file is to be considered by Info-CMemR for permanent preservation it should normally be sent to the relevant archive within 5 years of its closure. Files which also have ongoing administrative value may be retained locally for an extended period and should be forwarded to Info-CMemR when they are no longer needed. However, Info-CMemR must be advised in writing of any case in which the file is still required by the business unit for administrative purposes 25 years after closure.

If the MOD Form 262F recommends that the file can be destroyed locally it may be retained by the business unit for up to 25 years after its closure. If the file has not been destroyed within 25 years of its closure permission must be sought from Info-CMemR to retain it.

Files which are to be retained for an extended period for administrative purposes and are likely to be consulted on a frequent basis but which are not considered to merit permanent preservation may be forwarded to the relevant local archive for storage if there is sufficient storage space. However if local storage space is at a premium then to keep the subsequent retrieval costs down, low usage files should be sent to the relevant archive instead. In these circumstances the records officer must ensure that explicit reasons are given on the MOD Form 262F for the ongoing retention of the file.  Failure to do so may result in the file being destroyed by Info-CMemR.

### 4.9 Retention of Other Records

Unregistered records which merit consideration by Info-CMemR for permanent preservation are to be forwarded within 25 years of their creation, in accordance with the instructions in Chapter 7. Info-CMemR must be advised in writing of any case in which such records are still required by the business unit for administrative purposes 25 years after closure.

Unregistered records required for administrative purposes may be retained by the business unit for up to 25 years after their creation. If the records have not been destroyed within 25 years permission must be sought from Info-CMemR to retain them.

Unregistered records which are to be retained for an extended period for administrative purposes may, by prior arrangement, be forwarded to the relevant archive for storage if there is insufficient storage space within the business unit.

### 4.10 Maintaining the MOD Form 262A and MOD Form 262F

When a file is destroyed by the business unit the MOD Form 262F is to be removed and used to replace the Registered File Record Sheet (MOD Form 262A) which should then be destroyed.

If the file is not destroyed locally but is forwarded to the relevant archive the original MOD Form 262F must accompany the file. The business unit should retain a copy of the MOD Form 262F, annotate it to indicate that the file has been forwarded to the relevant archive and use it to replace the MOD Form 262A which should be destroyed.

The MOD Form 262A and MOD Form 262F are the definitive record of a file's existence and subsequent destruction/passage to the relevant archive. MOD Form 262A must not be destroyed until replaced by MOD Form 262F. Each MOD Form 262F must be retained for a period of not less than 30 years from the date of last enclosure (as recorded on the form). As MOD Form 262Fs are normally retained in a binder relating to a file series or a number of file series the binder should normally be retained for a period of not less than 30 years following the insertion of the final MOD Form 262F. If a business unit is disbanded during this period the binder(s) should pass to the successor business unit. If there is no successor business unit the binder(s) should be forwarded to the relevant archive.

### 4.11 Sponsors of Manuals and Books of Reference

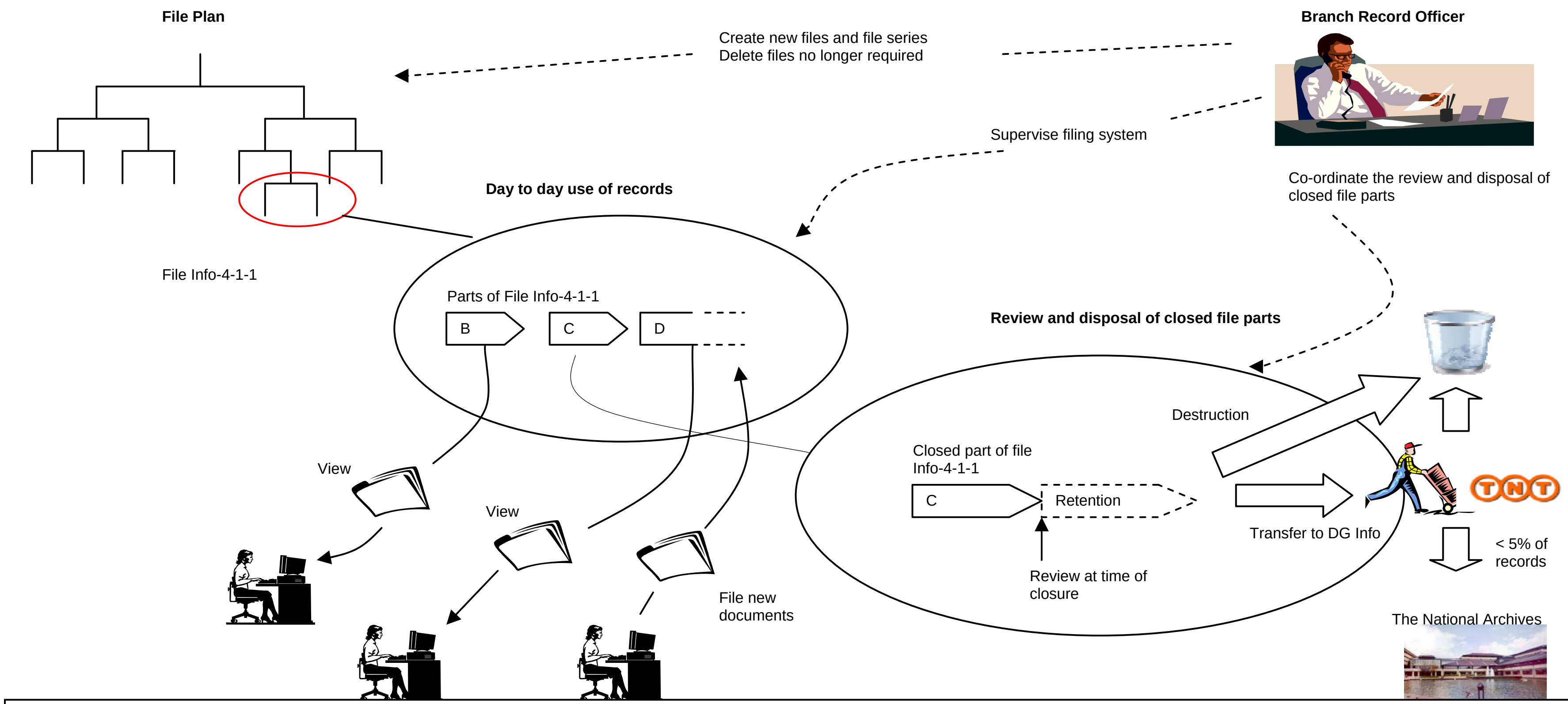
Sponsors of books of reference, manuals, directories, etc. are to ensure that a copy of the material is forwarded to the relevant archive for consideration for permanent preservation. Sponsors are to maintain an un-amended copy of each publication together with loose copies of each amendment for this purpose. Such material should be forwarded to Info-CMemR in accordance with the instructions in Chapter 7.

### 4.12 Destruction of TOP SECRET Registered Files and Files Containing Codeword Material

All registered files containing TOP SECRET and/or codeword material are to be forwarded to Info-CMemR in accordance with the instructions in Chapter 7, even if the Registered File Disposal Form recommends that the file should be destroyed.

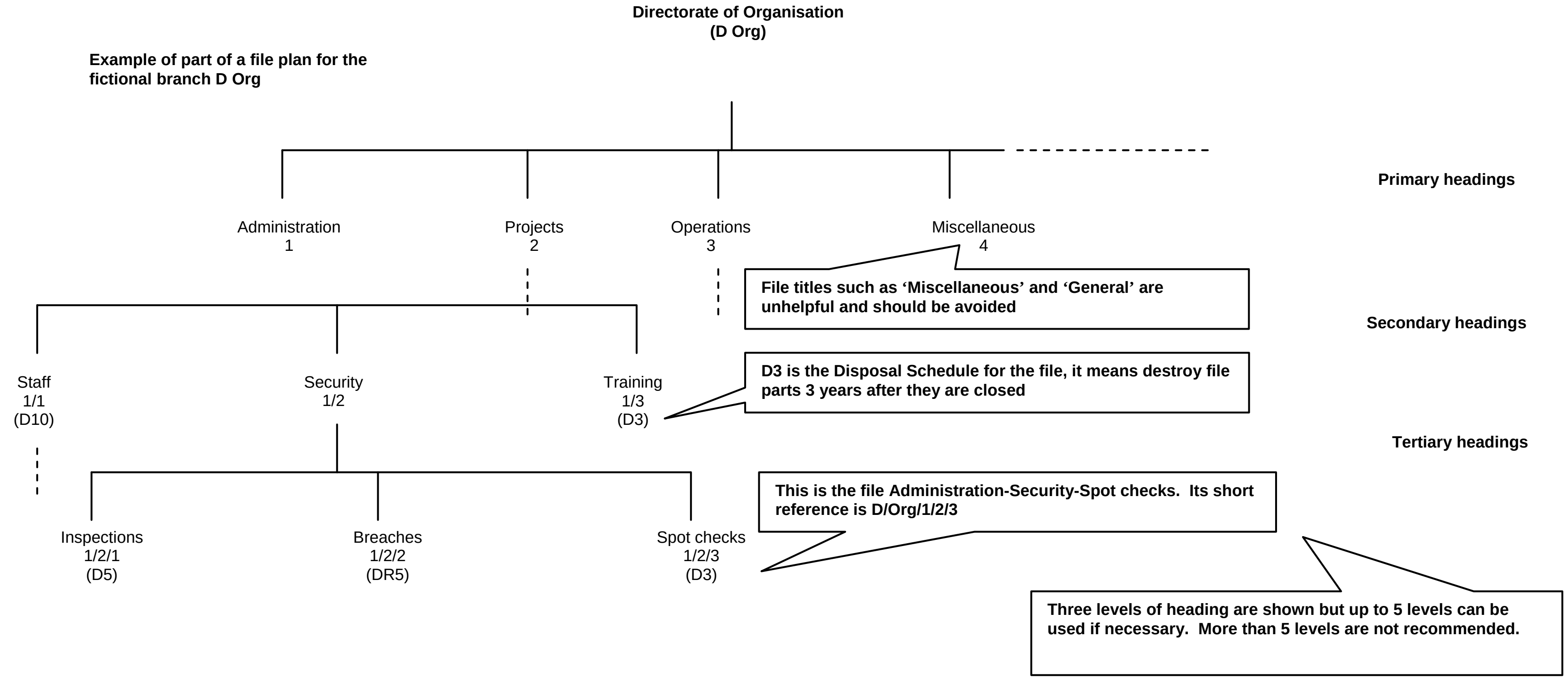
# Chapter 4 - Annex A

## Record Management Overview


File Plan
Branch Record Officer
Create new files and file series
Delete files no longer required
Supervise filing system
Co-ordinate the review and disposal of closed file parts
Day to day use of records
File Info-4-1-1
Parts of File Info-4-1-1
B
C
D
View
View
File new documents
Review and disposal of closed file parts
Destruction
Closed part of file Info-4-1-1
C
Retention
Review at time of closure
Transfer to DG Info
TNT
< 5% of records
The National Archives

**Notes:**

- This diagram shows three key aspects of record management: file plan management, day-to-day use of records and the review and disposal of records
- Most users of records are only involved in filing new records or viewing records which they or others have filed.
- The Branch Records Officer (BRO) is responsible for creating and maintaining the file plan, ensuring that the filing system is being used correctly, ensuring that file parts are closed and reviewed in a timely manner and disposed of as soon as their recommended retention period has expired.
- These activities are explained in more detail in the following diagrams.



**File titles such as ‘Miscellaneous’ and ‘General’ are unhelpful and should be avoided**

**D3 is the Disposal Schedule for the file, it means destroy file parts 3 years after they are closed**

**This is the file Administration-Security-Spot checks. Its short reference is D/Org/1/2/3**

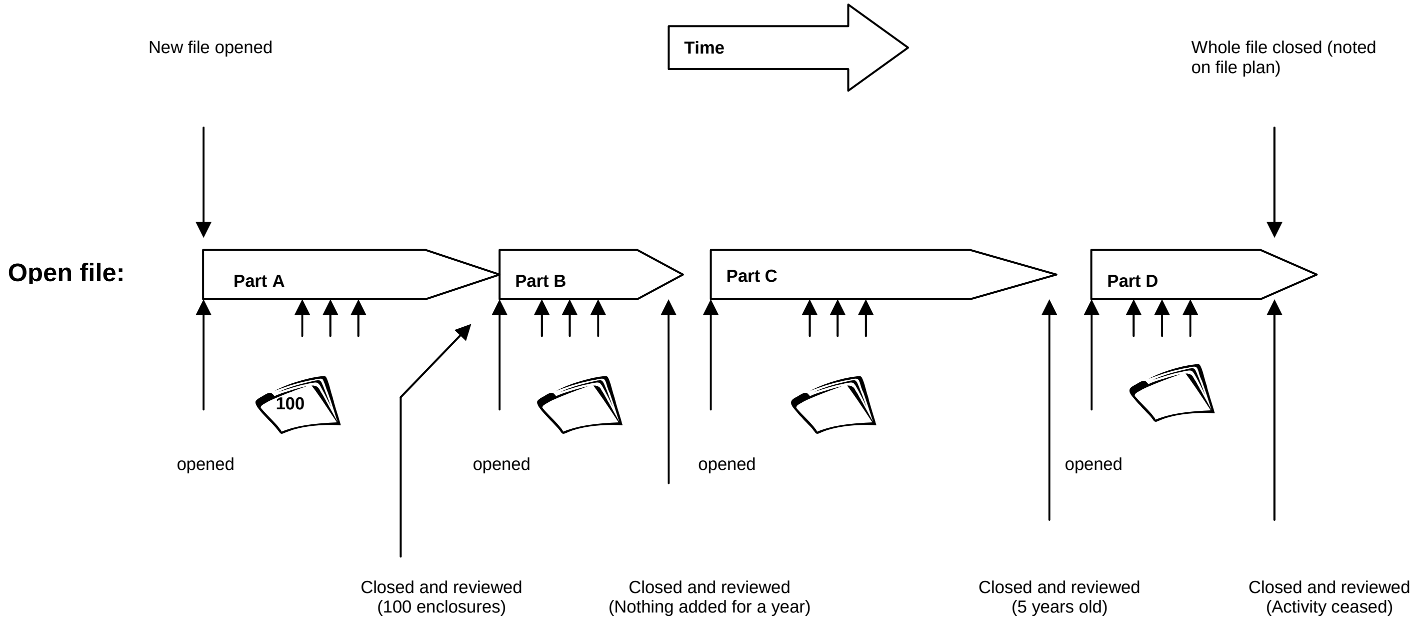
**Three levels of heading are shown but up to 5 levels can be used if necessary. More than 5 levels are not recommended.**

## Notes:

- A good file plan is usually based on the structure and functions of the organisation that it serves.
- Each file should have a numerical reference.
- Each file should have a disposal schedule recommendation associated with it to show when file parts should be destroyed or passed to DG Info for consideration for permanent preservation.
- New file plans must be approved by Info-CMemR who can also give guidance on construction of file plans.

**Keep the file plan logical and simple.**

## THE LIFE OF AN OPEN FILE


New file opened
Time
Whole file closed (noted on file plan)
Open file:
Part A
Part B
Part C
Part D
100
opened
opened
opened
opened
Closed and reviewed (100 enclosures)
Closed and reviewed (Nothing added for a year)
Closed and reviewed (5 years old)
Closed and reviewed (Activity ceased)

**Notes:**

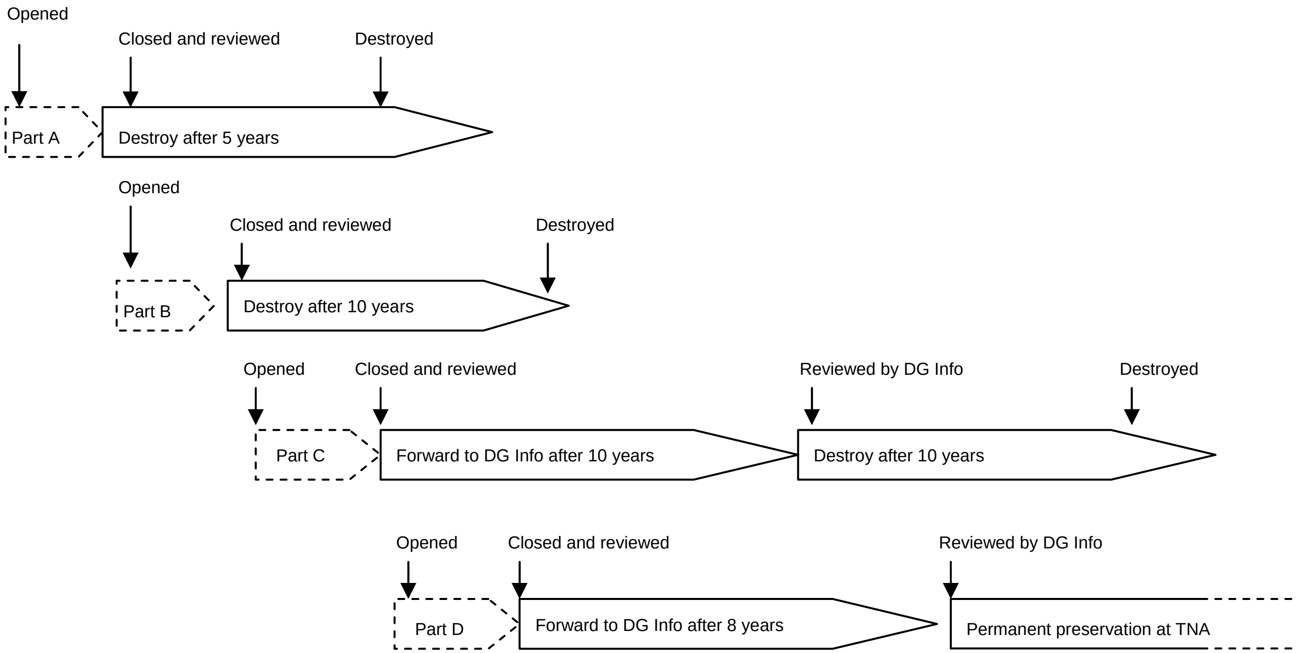
-Here is the life-cycle of a typical open file which over time needs to be split into four parts A, B, C and D

-Each new part is only opened when there is an enclosure to file on it. Note that this can result in time gaps between the parts.

-Parts are closed for several reasons: 100 enclosures (Part A), nothing added for a year (Part B), the part is 5 years old (Part C).

-Eventually the activity associated with the file totally ceases so there is no longer a need for the file. Its final part (Part D) Is closed and the whole file is recorded as closed on the file plan.

## THE LIFE OF A CLOSED FILE



**Notes:**

- Here is the life-cycle of a closed file. Its disposal schedule recommends local destruction 5 years after closure.
- Over time the file's four parts A, B, C and D are disposed of in various ways. **NB: In practice it would be highly unusual for parts of the same file to have such widely differing disposals. This example is for illustration only.**
- Part A follows the disposal schedule recommendation and is destroyed 5 years after closure.
- At Part B the reviewer decides to extend the retention period to 10 years at which point the file part is destroyed.
- At Part C the reviewer decides to transfer the file part to DG Information as it may merit permanent preservation. The DG Information reviewer decides that permanent preservation is not merited and marks the file for destruction after a further 10 years.
- At Part D the reviewer decides to transfer the file part to DG Information as it may merit permanent preservation. The DG Information reviewer agrees that permanent preservation is merited and arranges transfer to the TNA.

# Chapter 4 - Annex B

## Example of a Completed Disposal Schedule

| Ref No. | Main Heading | Secondary Heading | Tertiary Heading | Disposal Schedule Recommendation |
|---|---|---|---|---|
| 1.1.1<br>1.1.2<br>1.1.3 | Administration | Personnel | Training Plans<br>Investors in People<br>Equal Opportunities | D5<br>D3<br>D5 |
| 1.2.1<br>1.2.2 | | Health & Safety | SHE Plan<br>SHE Network | D5<br>D3 |
| 1.3.1<br>1.3.2 | | Equipment | Asset Registers<br>Maintenance | D10 RL2<br>D6 RL2 |
| 2.1<br>2.2<br>2.3 | Security | BSO Network<br>Clearances<br>Visits | N/A | D5<br>PP RL5<br>D10 RL2 |
| 3.1<br>3.2<br>3.3 | Finance | Budget<br>Structure<br>RAB Policy | N/A | PP RL5<br>D10 RL2<br>D5 |

Destroy locally 5 years after closure

Destroy 10 years after closure – retain locally for 2 years then pass to relevant archive

Pass to relevant archive with a recommendation that file part be considered for permanent preservation but retain locally for 5 years

a. The above is an example of an extract of a completed Disposal Schedule. In this example, the records are contained in registered files. The schedule should also include any unregistered records

b. Note that the schedule identifies each Main Heading and then each subordinate heading by number and title. Each individual file is then listed under the appropriate headings. In this example most files have a three part title (main, secondary and tertiary headings).

c. Variations on three abbreviations can be used to record all relevant disposal recommendations:

(i.) **D** = retain locally and destroy * years after closure (Note that the D prefix **must** be accompanied by the relevant timescale as in the example **2/1** above where "**D5**" denotes "destroy 5 years after date of last enclosure").

(ii.) **PP** = pass to Info-CMemR with a recommendation that the file merits consideration for permanent preservation. File **3/1** is an example of a file that has been identified as meriting such action.

(iii.) **RL** = retain locally for a period of time before passage to Info-CMemR for storage or review. (e.g. file **1/3/1** has been annotated "**D10 RL3**" to denote "to be destroyed 10 years after date of last enclosure but retained locally only for 2 years, after which the file will be forwarded to Info-CMemR for storage.").

d. Each business unit should give consideration as to whether to introduce a blanket policy whereby files which are not marked for early destruction should be passed to Info-CMemR for storage after a specified period (perhaps 2 years after date of last enclosure). Such a policy reflects the fact that most files will not be needed on a regular basis after this period of time and should not be occupying valuable and limited local storage space. Where necessary such files can be called back for reference.

e. Where it is not possible to make a recommendation about the disposal of a file the abbreviation NR (no recommendation) is to be used. The records officer/desk officer will need to consider such a file on its merits at the time of file review. Such a course of action should be unusual.

# Chapter 4 - Annex C

## Guidance on how long to keep records

1. **Contracts**

The legislation underpinning the retention of records relating to contracts is the Limitation Act 1980. Other relevant statutes include:-

- Unfair Contract Terms Act 1977.
- Latent Damage Act 1986.
- Consumer Protection Act 1987.

The Limitation Act, which applies to proceedings by and against the Crown, has the effect that proceedings to recover money must be instituted within six years of the money becoming due. The direct effect of the Limitation Act is therefore that many contractual records need to be retained for 6 years after the end of the contract. (Some special contracts are executed under seal and the limitation period in these cases is 12 years.)

Records relating to contracts worth less than £5,000 should be destroyed no later than two years after their creation.

Major policy developments and associated contractual files require special care during appraisal. All records relating to the same issue must be reviewed using the same criteria. For example, some contractual files might be retained alongside related policy files until final destruction or onward passage to the Public Record Office (PRO).

Some departments are choosing to transfer paper records to other media e.g. digital form (see also Chapter 5 below). In these cases branches must comply with requirements laid down in the British Standards Institute (BSI), Business Information Publications (BIP) 0008 - Code of Practice for Legal Admissibility (BIP 0008) and Evidential Weight of Information Stored Electronically and BSI DISC PD 0010 - Principles of Good Practice for Information Management.

2. **Accounting Records**

Government departments' and agencies' accounts (Vote Accounts and Trading Accounts) have to be laid before Parliament and are therefore preserved as published Parliamentary papers. These published accounts are sufficient for most future research purposes and therefore supporting documentation may be destroyed after any limitation periods have expired.

Statutes that may bear on retention periods for documents of various departments and agencies are:-

- Civil Evidence Act 1995.
- Value Added Tax Act 1994.
- Companies Acts 1985 and 1989.
- Consumer Protection Act 1987.
- Data Protection Act 1984.

- Financial Services Act 1986.
- Limitation Act 1980.

Branches operating specialised accounts or funds should consult their own legal branches, or relevant legislation, to determine if special provisions for the retention of documents apply.

All retention periods are given in whole years and should be computed from the end of the financial year to which the records relate. The retention periods cited are based in the general National Audit Office (NAO) requirement that main accounting ledgers should be retained for six years and supporting documents for eighteen months following the end of the financial year to which they relate. For administrative convenience we have substituted two years in the advice given instead of the eighteen months stated by NAO.

**Cheques**

| | |
|---|---|
| Cheque book/butts for all accounts | 2 years |
| Cancelled cheques | 2 years |
| Dishonoured cheques | 2 years |
| Fresh cheques | 6 years |
| Paid cheques | 6 years |
| Cheque stoppages | 2 years |
| Cheque registers | 2 years |

**Bank Details**

| | |
|---|---|
| Bank deposit books/slips/butts | 2 years |
| Bank deposit summary sheets | 2 years |
| Bank statements | 2 years |
| Certificates of balance | 2 years |

**Other Records**

| | |
|---|---|
| Expenditure sheets | 6 years |

| | |
|---|---|
| Cash books | 6 years |
| Petty cash receipts | 2 years |
| Creditors’ history records | 6 years |
| Statements of outstanding accounts | 2 years |
| Credit notes | 2 years |
| Debit note books | 2 years |
| Claims for payment | 6 years |
| Purchase orders | 6 years |
| Accounts payable (invoices) | 6 years |
| Wages | 6 years |
| Cost cards / costing records | 2 years |
| Creditors’ ledgers | 6 years |
| Prime records for raising of charges | 6 years |
| Year-end balances/published accounts | 6 years |
| Postal records / books | 6 years |
| VAT receipt books | 6 years |
| Debts/overpayments/write-offs | 6 years |
| Employee pay histories | 6 years |
| Leaving staff | Keep last 3 years records for pension calculations |
| Salary rates register | As superseded |
| Stores inwards books | 6 years |
| Stock control | 2 years |

| | |
|---|---|
| Purchase orders | 6 years |
| Travel warrants | 2 years |
| Requisition records | 2 years |
| All asset registers | 6 years after last entry is disposed of |

3. **Building Records**

This guidance covers all buildings on the Government Estate and is supported by English Heritage (Conservation Unit). All records of construction and works processes, including plans and drawings, of Government buildings are public records within the meaning of the Public Records Act 1958.

Where records have been created by a private contractor in fulfilment of a contract that has been let by a Government department or agency, these are also public records excepting those records relating to the internal administration of the contractor, e.g. personnel and wages records. Government building records are varied but, for the purposes of this guidance, are divided into three broad types: Legal, Policy and Administrative.

4. **Health & Safety Records**

Because health and safety records may be kept in different parts of an organisation, communication across the organisation and between the Department Record Officer and Health and Safety Manager is essential to ensure consistency in record keeping and disposal.

The legislation underpinning health and safety in the United Kingdom is the Health and Safety at Work Act 1974.

- The Social Security Act 1975 is also relevant to health and safety record keeping. Section 88(b) is the enabling provision under which relevant regulations are issued, such as the Social Security (Claims and Payments) Regulations 1979 and the Social Security (Industrial Injuries) (Prescribed Diseases) Regulations 1985.
- Other relevant legislation includes the Factories Act 1961 and the Fire Precautions Act 1971.

Records relating to health and safety matters will probably be held by different parts of the organisation. For example:-

- Reports of accidents or incidents effecting individuals should be kept on personal files.
- Finance departments will have records of the purchase of plant and equipment.
- Facilities management will have maintenance records.
- Security departments will maintain records relating to emergency evacuations.

Health and safety records are either required to fulfil a statutory obligation or may be needed as a prerequisite to carrying out certain activities. Failure to hold valid documents may attract the penalties of prosecution, improvement or prohibition notices. For example:-

- Failure to provide evidence of training on the use of dangerous machinery may attract an improvement notice.
- Failure to maintain a register of dangerous substances under the Control of Substances Hazardous to Health (COSHH) regulations may lead to a prohibition on using such substances.
- Inability to provide appropriate and accurate documentation in the event of civil litigation may lead to heavy compensation payments.

The Management of Health and Safety at Work Regulations 1999 requires pre-employment medical screening to determine whether someone can carry out a specific task without risk to their health and safety. Clearly, these records need to be kept for the duration, and after, the employee has carried out these tasks in case of claim for compensation.

Health and safety records might be kept for the following reasons:

- The documents are required by legislation.
- The operations or process may be used again and the records are needed to ensure safety.
- The documents may be used in litigation or prosecution.
- To demonstrate the department’s history of safety management.
- To identify long-term trends, plan maintenance, or identify training needs.

Under the Limitation Act 1980, personal injury actions must be commenced within three years of the injury. However, for some complaints, such as asbestos and noise damage, the employee may not realise he or she has contracted it until several years after exposure. In such cases the Act allows the claim to be brought within three years of the date that the employee had the knowledge of the disease or injury. It is recommended that relevant records be kept for 40 years for such incidents. Evidence that may be useful could include relevant risk assessments e.g. formal surveys of the workplace, safe operating procedures, effectiveness of controls e.g. monitoring of noise and/or light levels, maintenance records for machinery and medical surveillance e.g. pre-employment medicals and audiometry.

5. **Examples of Disposal Scheduling:**

Where exposure may lead to a disease many years later - keep the record 40 years after the last exposure.

- Health surveillance, including medical reports – keep the record 40 years from the date of the last entry.
- Accident book - 3 years from date of last entry.
- Health records - 50 years from date of last entry.

- Air monitoring – keep the records for a minimum of 5 years.
- Examination of respiratory protective equipment – keep the record for 2 years.

6. **Personnel Files**

For many years the recommended retention period for most documents has been 100 years from the date of birth. The main reason for this has been the requirements of the Principal Civil Service Scheme (PCSPS).

Personal security records should also be kept as separate annual sub-sets of personal files. The Guide to Personnel Security (GPS) suggests that these records should be kept until 5 years after leaving – if the person leaves at normal retirement age – or 10 years if he/she leaves before normal retirement age (GPS paragraph 5.1). The annual files should be destroyed after 10 years except where a security breach case is in action.

Medical records should be kept as separate annual sub-sets of personal files.

Departmental health and safety issues potentially affecting multiple members of staff, such as records under:

- Control of Substances Hazardous to Health (COSHH) regulations
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR)

- should be documented on departments’ administration or subject files (cross-references from these files to those of likely effected staff would be useful). Medical sub-files should be destroyed after 10 years except where a case is in action with the Civil Service Occupational Health Service or where a member of staff, or their Trade Union/Legal Representative, has initiated legal action against the department.

Monthly payment of pay records can be kept as separate annual sub-sets of personal files and destroyed on a rolling basis after 3 years. Pension entitlement may be captured in paper or digital form and amended as necessary during the working life of the employee. This record must contain the appropriate endorsements by authorised personnel to ensure eligibility and authenticity is maintained. If pension entitlement is not captured in a single rolling record all documents bearing an entitlement must be retained until 72 years from date of birth or 5 years from last action, whichever is the later.

Personnel papers not within the foregoing sub-sets should be destroyed 3 years following resignation or retirement.

# Chapter 5

## Electronic Records Management in MOD

### 5.1 Introduction

This chapter addresses the policy and practice for the management of electronic records. It is applicable to all existing and future record collections in the MOD. The policy for the management of records, in general, is the same for both physical, i.e. paper, and electronic records. This chapter should therefore be read in conjunction with the rest of JSP 441 for a complete overview of the general principles of records management.

Chapter 5 Part A sets out the Corporate Electronic Records Management (ERM) Policy and corresponding guidance for those using a formal Electronic Records Management System (ERMS). Part B deals with policy and guidance for users without an ERMS capability approved by The National Archives (TNA).

This policy covers electronic records containing any type of information held within MOD[2], at all levels of sensitivity. This policy addresses:

- the requirements that must be met for the electronic records themselves to be considered as a proper record of activities undertaken by the department, and as sufficient evidence to support decisions taken
- the requirements for electronic records systems, and the processes required to ensure the quality and reliability of records as a valuable corporate information resource

Annex A provides instructions for project teams introducing an ERMS. As most of the MOD will get ERMS capability when the Defence Information Infrastructure (DII) is rolled out, these instructions will only apply to project teams introducing ERMS in areas **not** provided with DII.

### 5.2 Applicability

This chapter applies to staff in the following roles:

Users[3]

Users are responsible, in the course of their normal business for activities such as:

- Identification of electronic documents appropriate for declaration as electronic records, because of their business function or content.
- Creation of electronic records, capturing all consistent and reliable contextual information, as well as adequate metadata[4] describing the record.

[2] The terms ‘MOD’ and ‘Department’ as used in this document refer to the whole Ministry of Defence, its Trading Funds, Agencies and the Armed Forces.

[3] Those who, at all levels of a Unit, generate and use electronic documents in their daily activities.

- Declaration of electronic records that document the activities of the business.
- Appropriate use of existing records in support of current business activities i.e.: FOI requests, lessons learnt and co-operation with any audit trail mechanism.

Information Management (IM) Staff[5]

IM staff are responsible for the management of both physical and electronic records. As regards ERM, this involves:

- Setting local electronic records policy.
- Enforcing proper electronic records management procedures.
- Supporting users within their business/operational unit (hereafter a Unit).
- Management of their Unit's information resources, i.e. its records and, in particular, for structuring the unit's environment in which the proper capture, maintenance and disposition of electronic records takes place (e.g. creating file plans, applying disposal schedules).
- The continued management of physical records according to their schedule for retention.
- Phasing out the use of physical records when ERMS are in place.
- Preparation of electronic records for migration from one information system to another, and safekeeping of these records during the migration process.
- Developing knowledge about ERMS functionality, technical operation and processing.
- Ensuring that retention schedules are appropriately allocated following consultation with the Corporate Memory ERM team (Info-CMemERM).
- Disposal of those electronic records no longer required, following consultation with subject matter experts (SMEs).

## 5.3 Further Guidance

For practical guidance on ERM and ways of working, users should, in the first instance, consult their local user guide/iHub guide/other relevant documentation. Please contact your local IM for more information.

Info-CMemERM can provide advice and assistance with the general application of this Chapter, or related ERM topics. Any practical difficulties experienced in applying these instructions should be reported to Info-CMemERM.

[4] Metadata is usually defined literally, as '*data about data*'. It is the descriptive information held with a record to enable reliable retrieval and future management (See paragraph 5.6).

[5] The term 'IM staff' used in this context covers all those who support information management as part of their role. This includes, but is not limited to; Information Managers (IMs), Information Support Officers (ISOs), Branch Record Officers (BROs), Information Administrators (I-Admin), Senior Information Officers (SIOs) and Records Managers (RMs).

## Corporate Policy for Electronic Records

### 5.4 Background

Good record keeping is essential for many reasons, most importantly because it supports daily business within the organisations that create records. Good record keeping is also necessary as it supports the wider departmental need for information - including compliance with the Public Records Acts, DPA and FOI and enables the Department to respond to challenges and support its actions.

Electronic records have many advantages over conventional paper record keeping systems. They:

- Improve the efficiency of business processes that utilise records.
- Allow information to be shared across a wider community.
- Allow faster and more effective access to information.
- Save storage space.

It is the aim for the whole of MOD to share a common ERMS, and to this end, a common capability will be rolled out on the DII. Adherence to a single policy will support this move towards coherence, and help ensure that good quality records are produced, managed and shared across MOD.

# Part A – Policy & Guidance for Electronic Record-Keeping in an Electronic Records Management System (ERMS)

### 5.5 All newly created records will be stored and managed electronically in an approved online ERMS.

An ERMS supports the preservation, for as long as necessary (and no longer), of the records generated by, or used by, a Unit. These records should provide evidence of the activities that took place, establish exactly what happened and enable others to understand why decisions were taken. Records must be seen to be trustworthy. In our increasingly litigious society they may be required to substantiate or refute legal claims and it may be necessary to demonstrate their authenticity and integrity in a court of law. Good ERM practice will ensure that through time records:

- Are present.
- Can be accessed by those entitled.
- Can be understood.
- Can be trusted (as being authentic).
- Can be deleted when no longer required.

As soon as a document is chosen for preservation – short or long term - it becomes a part of the Department's record and then, by definition, it is immutable, i.e. it must not be amended, and must be managed in a suitable environment to support its preservation. In the electronic world, this can only be achieved by storing the record in an approved ERMS.

The underlying principle is that staff must ensure that they maintain a proper record of business by declaring all relevant information, including e-mails, electronic documents, etc. as records in their ERMS. All papers of substance must be captured into an ERMS. Ephemeral papers, rough drafts, spare copies etc. need not be captured if they are likely to be needed only temporarily and are not of any lasting significance.

When capturing records into an ERMS, it is vital that the appropriate records are captured. Units must ensure that users have a clear understanding of the information that should be captured as a record. Chapter 4 Annex C gives examples of records likely to warrant permanent preservation.

### 5.6 Electronic Records must contain adequate metadata

Metadata is usually defined as 'data about data'. It is the descriptive information held with a record to enable reliable retrieval and future management. Metadata for normal letters and minutes would typically include title, creator, date created and addressee; however the range of metadata held depends on the type of information in the record. For example, geographical co-ordinates might be essential metadata for a map but totally meaningless for an invoice.

When declaring a record into the ERMS, basic metadata is captured automatically by the system. However, users must ensure that sufficient metadata is captured to provide the information necessary to serve a number of different purposes.  Metadata:

- Establishes the context in which the record was created, received and used.
- Provides information to indicate whether the records integrity is intact, i.e. that it has not been subject to changes after being declared.
- Provides an adequate description of the record itself.
- Supports the retrieval of, and access to, the record by a range of users.
- Retains contextual information about the record and enables its future interpretation.
- Provides essential information to maintain the record over time and through changes in technology.

At the time of declaring a record, the content and most of the applicable metadata is fixed as it is at that point, and cannot be changed.  There are, however, some metadata elements such as 'Protective Marking' and the various disclosability markers (e.g. FOI releasability) that may be amended throughout the life of a record.

Once captured into an ERMS the success, or otherwise, of a search will depend in part on the type of information stored and its associated metadata.

### 5.7 Self Modifying Fields

Records with self modifying fields, e.g. a date field that automatically updates to reflect real time, will not display correct information when the record is viewed in future.

Users must not declare records that contain self modifying fields into the ERMS.

### 5.8 Reference Material

Any information referenced within a record (e.g. within the text or as a footnote) should itself be accessible in the correct version and format.  If there is any doubt as to the accessibility of the referenced material, then that material should be filed into the same folder as the record for coherence.

If you as a business unit make decisions based on 3rd party material that you refer to but have no control over or cannot guarantee future access to, then it is your responsibility to declare that material (subject to copyright) as a record.

### 5.9 Folder Level Metadata

Folder level metadata identifies the attributes that apply to whole groups of records. This metadata serves four main functions of electronic records management:

- Grouping records together: providing an identifying label under which similar records can be grouped together, and which distinguishes separate groups from each other.
- Showing how groups relate to each other: enabling a linking structure that can show the place of one group within the wider semantic structure of the file plan.
- Enabling management of the group of records as a whole: so that the records can be retained, scheduled and disposed of as a consistent group.
- Enabling access to the group of records as a whole: to demonstrate the narrative context in which records should be understood.

Folder level metadata can also be used to link together conventional paper and electronic filing structures, where these are not in themselves identical, and are an essential element in linking hybrid assemblies where electronic and paper records are contained in one folder.

Folder level metadata (usually through the use of audit logs) must be retained after a folder part has been destroyed for a minimum period of 30 years, to document the action that was taken on the records as part of the formal scheduling process. The proof that a folder part and its contents have been reliably destroyed can be invaluable in answering queries particularly requests raised under DPA and FOI legislation.

### 5.10 Records will be managed within the creating Unit for the duration of their lifecycle, unless otherwise agreed by Info-CMemERM

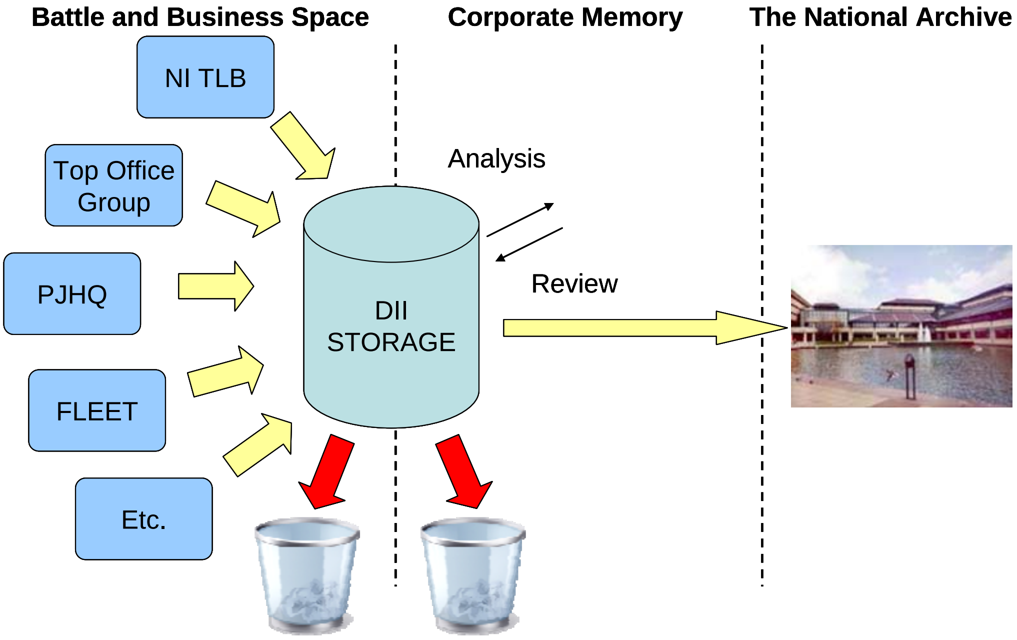
Most records lose their importance over time and many are only needed in the short-term. However, they are still vital for carrying out day-to-day business in the Unit that created them, and some may be of interest to the nation generally and to individual members of the public.

Individual units are therefore responsible for the through-life management of the majority of electronic records that they create. This involves the Unit's IM staff managing access, retention and the ultimate disposal of the records. When a Unit ceases to exist, and its information is still required for business use, Info-CMemERM may take responsibility for the management of the records.

Whilst many of the records we create will eventually be deleted, a small minority of records will require long-term retention for corporate use, and may ultimately be worthy of permanent preservation at TNA. Info-CMemERM will also take ownership of these selected "key" records, which will be accessible to both their creating Unit and Corporate Memory for as long as necessary.

This diagram shows the way in which MOD's electronic records will be managed, and the ownership of these records at various stages in their lifecycle:

## Diagram - Through-Life Ownership of Electronic Records



### 5.11 Electronic records will be organised within a file plan, which must be submitted to Info-CMemERM for approval

ERMS file plans define a hierarchical filing structure into which individual records are filed. A good file plan should be intuitive and should simplify the tasks of deciding where to register a particular record. It should also assist the decisions regarding the review, retention and disposal of folders.

A single file plan should be used for all records held in, or tracked by the ERMS irrespective of the media (e.g. electronic, paper, optical, film) on which they are held.

The structure of a filing system used for electronic records should closely follow the guidance for paper records defined in Chapter 3.

Local file plans within the ERMS will be created by the Unit IM staff following Info-CMemR guidance as described in Chapter 3.

Only IM staff should be able to open a new electronic class, folder or folder part. Info-CMemERM must approve the main headings, numbers and structure of all MOD file plans before implementation on an ERMS.

Within Unit file plans, Corporate Memory Records team (Info-CMemR) will earmark any sections that are of specific long-term interest at Departmental level as ‘key’. These “key” sections will fall under Corporate Memory ownership; the Unit will continue to manage and access the records for as long as they are needed locally.  The IM staff must not modify the contents once the part has closed to allow for Info-CMemR review.

Local review/disposal of records must not be carried out on contents of “key” folders. IM staff must liaise with Info-CMemERM regarding any disposal action.

The minimum metadata that IM staff must ensure is applied to all classes, folders and folder parts in a file plan at the point of creation is given below:

| REQUIRED METADATA | Comment |
|---|---|
| Identifier. System ID | Unique reference number, automatically generated by system |
| Identifier. File plan ID | Identifier for a file plan object. Derived from the file plan itself e.g. DG Info-4-1-1 |
| Title. Title | Meaningful name given to the object |
| Date. Opened | Date the folder/part was made available for records to be declared |
| Date. Closed | Date on which further additions were prevented |
| Aggregation | Defines the required data at each level. System generated |
| Relation. Has Part | Identifies instances where the content of a record has a direct relationship with that of another or clarifies how one level of aggregation relates to other levels |
| Subject. Category | From the Defence Taxonomy |
| Subject. Keyword | From the Defence Thesaurus |
| Security. UK Protective Marking | Allows automation of restrictions and permissions to view records e.g. RESTRICTED |
| Security. National Caveats | Additional protection for protectively marked material e.g. UK EYES ONLY |
| Security. Descriptors | Identifies the nature of the sensitive information e.g. SECRET-MANAGEMENT |
| Disposal. Disposal Schedule ID | Unique identifier of disposal schedule applied e.g. D5 *(See Chapter 4 Annex B)* |

Records should not be transferred between electronic folders unless they have been misfiled. All record transfers of this type must be registered on the ERMS audit log. The audit must capture (in metadata/comments) the individual who performed the transfer, the date of transfer, the record reference and the identities of the source and destination folders.

Folder parts are to be used to ensure that electronic files remain under management control.

**Folder parts should be set to close after 100 enclosures AND/OR annually, at the end of each calendar year (whichever happens sooner).** This will aid cross-Departmental thematic review, and allow related records held on different systems (for example at different levels of protective marking) to be linked.

A new folder part should not be opened unless there is likely to be an imminent need to file new enclosures. IM staff may wish to consider closing the electronic folder altogether if it seems likely that it has no further value.

**5.12 Within the electronic file plan, every class and/or folder will bear a retention schedule that has been approved by Info-CMemERM**

Retention Schedules are an essential feature of all ERMS. They ensure that folders are reviewed (usually after a period of years) to determine the appropriate disposal action to be taken on that folder. Schedules can also be assigned to series and hierarchies of folders and inherited as defaults from higher-level folders.

The creating Unit’s IM staff must ensure that appropriate retention schedules are set for each class/folder in the hierarchy.
Info-CMemERM will review/approve all retention schedules, in order to identify “key” areas that may contain records that have long-term value or are worthy of permanent preservation.

Most ERMS will contain a series of pre-defined retention schedules, from which IM staff, in consultation with the subject matter expert (SME), can select the most appropriate. If no retention schedules have been defined, IM staff should contact Info-CMemERM for guidance.

It should be noted that in exceptional circumstances, e.g. where the defined retention schedule is too short, Info-CMemERM reserves the authority to override any local decisions.

When a folder part is closed the IM staff must ensure that the following metadata fields are captured in the folder’s metadata:

| REQUIRED METADATA | Comment |
|---|---|
| Identifier. System ID | Unique reference number, automatically generated by system |

| | |
|---|---|
| Identifier. File plan ID | Identifier for a file plan object. Derived from the file plan itself e.g. DGInfo-4-1-1 |
| Title. Title | Meaningful name given to the object |
| Date. Opened | Date the folder/part was made available for records to be declared |
| Date. Closed | Date on which further additions were prevented |
| Disposal. Disposal Schedule ID | Unique identifier of disposal schedule applied e.g. D5 |
| Disposal. Disposal (due/effective) date | Date when action will be triggered e.g. If 'D5' – 5 yrs from file part closure |
| Disposal. Disposal authorised by | Name/role of individual who authorised disposal |
| Disposal. Comment (if applicable) | Any comments on reasons for disposal etc |

### 5.13 Review

Once closed, all electronic folder parts must be reviewed within the allocated timescales, and appropriate disposal action carried out

Mechanisms within the ERMS should ensure that folder parts are regularly closed, and that the IM staff are notified when a folder part is scheduled for review and further action.

Reviews of folder parts should be carried out by the relevant Desk Officer/SME (to be agreed locally). Disposal action must then be agreed with the Unit IM staff.

Units have delegated authority to review and destroy locally only those records that have no further administrative value to the Unit and have not been earmarked by Info-CMemERM as being worthy of long-term or possible permanent preservation (key classes/folders). In making such a determination, the following principles should be applied:

- When a folder part is due for review, the Unit IM staff must consider whether the original disposal action is still valid. They will need to consult SMEs within the Unit, and may seek guidance from Info-CMemERM to come to a decision.
- Local deletion should only be considered for folders containing records of short-term/solely local value, e.g. those folders that relate to the administration of the Unit. If in doubt, contact Info-CMemERM for advice.

- All policy folders are of potential long-term value to MOD and Units should therefore consider consulting with Info-CMemR to determine any possible long-term/corporate value.
- If the SME decides that a folder part should be deleted, IM staff should action the deletion as soon as the retention schedule has expired.

The practice of ‘weeding’ electronic folders (i.e. selectively deleting enclosures) is expressly forbidden for the reasons given at Chapter 5.13. Only complete folder parts can be deleted.
TOP SECRET and Codeword electronic folders must not be reviewed or deleted locally. Info-CMemERM should be notified of their existence (and any disposal recommendations) so that appropriate action can be taken.

Info-CMemR will review “key” electronic records that may be considered worthy of long-term/corporate use or permanent preservation following procedures similar to those for paper records at Chapter.

Chapter 4 Annex C gives examples of records likely to warrant permanent preservation.

**5.14 Disposal**

For wholly electronic folders, there is no requirement to maintain Registered File Records Sheets (MOD Form 262A) or Registered File Disposal Forms (MOD Form 262F) as the details of the files existence and final disposition are held in the ERMS metadata.

If an electronic folder in an ERMS is used to track physical records, then the action at Chapter 3.23 and 3.24 for closing registered files also needs to be taken. A MOD Form 262F will also be required for the physical file part of a hybrid folder.

It is expected that Units will retain their electronic records within their own area of the ERMS.  Other than for key records, Info-CMemERM will only take responsibility of a Unit’s records if the Unit is being disbanded.

Units wishing to forward records to Corporate Memory in electronic form should, in the first instance, contact Info-CMemERM to discuss their requirement.

**5.15 Records held in an ERMS must be accessible to all users who are entitled to see them.**

The following paragraphs address confidentiality only in terms of access management and are not intended to replace the Department’s existing security policy promulgated in JSP 440.

A feature of ERMS is its ability to increase the availability of corporate information, providing a richer and more accessible information base for the conduct of Departmental business. As far as possible, records should be treated as corporate resources, and made available as widely as possible.

However, there will still be a need to restrict some forms of access to certain material e.g. to defined user groups/individuals in order to enforce national security, sensitivity and ‘need to know’ requirements.

All ERMS provide facilities for the allocation of rights in an access control table, and the attachment of these rights to classes, folders, or even individual records.

Applying the appropriate level of security to sensitive information is important and in general terms the information owner is responsible for determining its protective marking.

Working documents that have not been declared as records may have access controls placed upon them by their current owners, who wish to restrict availability of the document content for various reasons. However, once declared to the ERMS, the record comes under Departmental ownership and is governed by this JSP.

Any protective markings, caveats and descriptors associated with sensitive information should be applied to the information and held on the ERMS as metadata.

IM staff must identify relevant user groups within their Unit, and allocate broad functional rights to each group. These groups might include:

- Groups with access to higher levels of protectively marked records.
- Project teams or workgroups.
- IM staff/others who will manage record collections and metadata.

Functional rights that might be allocated in differing combinations to differing groups might include:

- Read/retrieval access to metadata or other record descriptions.
- Read/retrieval access to records contents.
- Edit rights to change the content of metadata or record descriptions.
- Read rights to make a physical copy of a record in order to create a new version.
- Records management rights to change the location of the record, or retention/scheduling information.

**5.16 Records held in an ERMS must be held in a format that allows continued access for the duration of their lifecycle.**

Most records stored within an ERMS are of short-term value, and will therefore be deleted within several years of their creation. However, some records will be required for much longer periods of time, whilst others will be kept in perpetuity.

Users/IM staff must ensure that all records declared to the ERMS are not encrypted, password protected etc. to ensure that they remain accessible for as long as required.

### 5.17 Cryptography

Definitive guidance on cryptography is available in JSP 440 and JSP 602: 1032 - Cryptography and Key Management. JSP 440 defines cryptography as being the art or science concerning the principles, means and methods for rendering plain text unintelligible, and for converting encrypted messages into an intelligible form.

This definition basically refers to the use of encryption/decryption to safeguard the confidentiality of documents and records, but it is also worth noting that cryptographic techniques are also used for Authentication (e.g. digital signatures) and Integrity (e.g. cryptographic checksums).

Records that are declared to an ERMS only in their encrypted form will be vulnerable to loss, for all effective purposes, once the means of encryption changes or is replaced.

> 📎 Encrypted documents must not be declared into an ERMS.
> They must be declared in their decrypted form.

### 5.18 Authenticity and Electronic (Digital) Signatures

This section deals with digital signatures. This should not be confused with “digitised signatures” which is a digitised representation of an individual’s own hand written signature. “Digitised signatures” are not recommended for use in MOD.

A digital signature is applied to a document through a cryptographic process using a private cryptographic key held, and accessible, only by the authorised user. The digital signature is applied to a hash of the data being signed by the private key. This means that if a digitally signed document is subsequently changed and not re-signed by original author, the signature will no longer be valid when cryptographically checked.

Digital signatures are verified (by a third party) using the public cryptographic key of the originator. If the signature verifies, it confirms two things:

a. That the document has not undergone alteration since being originally signed; and

b. That the identity of the signing party (originator) is the same as that shown on the certificate, thus the document can be considered genuine.

There are separate cryptographic key pairs for encryption and signing; however, the method in which digitally signed documents are stored is dependent upon the application in use.

In general, a digitally signed document can be stored in the EDRMS but must be in its native unencrypted (clear text) format.

The Defence Public Key Infrastructure (DPKI) will be adopted in DII across MOD. BROs and system administrators will need to be aware that to ensure access to records in the future, distinctions need to be made between:

- Those applications that use digital signatures but do not encrypt the content of the message hence it may be sufficient to document that the digital signature has been correctly assigned and authenticated; and

- Those applications that use some form of encryption on the message in order to ensure confidentiality, thus the record becomes inaccessible unless a decrypted version (or the means to obtain one) is available.

In general, a digitally signed document should be stored in the ERMS in its native unencrypted format along with the signature stating that it has been signed. It is also acceptable to store the certificate of the signer with the signed document to allow faster signature validation.

### 5.19 Electronic records/folders must be linked to any associated paper/physical media holdings

Along with storing the electronic records themselves, ERMS should be used to track related records in all forms including those on physical media such as charts, drawings, film reels, microfilm, magnetic tapes, CD/DVD ROMs and videocassettes.

Some active paper registered files are likely to exist alongside electronic record folders. In these circumstances the physical files will not be capable of fully duplicating their electronic equivalent, but their content will augment the electronic version. Together they combine to form hybrid folders.

If it is necessary to create a hybrid folder, it is important that the links between an electronic folder and its related paper file are clear to the users and easy to understand. Care must be taken to ensure that both the creators and future users of the records can easily identify this relationship, and that the accompanying metadata is maintained along with the electronic folder and records.

Where a decision is taken to maintain hybrid folders, the following procedures must be followed:

a. Enclosures held in the physical file must be maintained in strict date of origin order and must be allocated sequential enclosure numbers. Where enclosures are not received in date order, they should be inserted into the physical file accordance with the guidance laid down in Chapter 3.14.

b. The physical file itself must be managed in accordance with the guidance laid down at Chapter 3.

c. The metadata (including file name, physical file location, etc.) associated with the physical file must be declared into the ERMS to enable tracking.

d. A relationship between the contents of the physical file and the electronic folder must be created in the ERMS.

e. All enclosures from both the physical file and the electronic folder must be taken into account when decisions are made about the closure of the hybrid folder part.

f. The hybrid folder in its entirety is to be reviewed in line with the instructions in Chapter 4. If the hybrid folder is to be destroyed locally then both elements of the folder should be deleted. If the folder warrants transfer to Corporate Memory, then both elements of the file should be transferred.

### 5.20 Records must not be exported from the ERMS without prior

**authorisation from Info-CMemERM**

Any area that is considering exporting records from an ERMS to another Unit or an Other Government Department (OGD) must notify Info-CMemERM. In these circumstances, because of the possible conflicting aims of the different Units, there may be variations in the ERMS metadata. Close liaison between the importing and exporting areas will be required in order to enable the receipt of the incoming records.

Prior to exporting the information, all relevant folders should be closed with the metadata amended to provide details of the impending export. Since all of the relevant metadata will be automatically captured, the completion of a Registered File Record Sheet (MOD Form 262A) and Registered File Disposal Forms (MOD Form 262F) will not be required, however, for audit purposes, the exporting IM staff should retain details (a log) of all records that have been exported for 5 years, and the file plan annotated accordingly (unless of course the Unit is being disbanded). A copy of the log should be copied to the importing IM staff who will open the appropriate files in their file plan.

During the export of records from one ERMS to another, IM staff must ensure that the metadata for records that may have been previously deleted is also exported to the receiving system.

The imported folders should be closed and stored, with the original file plan structure preserved, in a separate area of the file plan from those files already on the system. New folders with different file plan numbers (File plan ID) to those previously imported can then be opened and metadata added to allow them to be cross-referenced with the old folders. The old folders must not have their file plan IDs re-numbered to match the new file plan.

The export of records from an ERMS by taking them offline is not recommended. However if manual export/import is necessary, please inform Info-CMemERM and refer to Chapter 5.37 for policy and guidance.

# Part B – Policy & Guidance for Electronic Record-Keeping in the Absence of an Electronic Records Management System (ERMS)

**5.21 Units choosing to maintain electronic records in the absence of an ERMS must ensure that business unit work in progress documents and records are managed separately. Info-CMemERM must approve all such systems.**

Most organisations in the MOD are dependent on electronic office automation systems. Although commonly used packages such as Microsoft Office support the creation and communication of electronic documents (Word documents, spreadsheets, calendars, email, etc.) they lack the capabilities required to preserve them as properly managed records. Such systems do not meet the standards of authenticity, integrity, reliability, security and accessibility necessary for the longer term needs of the originator, the Department in general, the courts, auditors and TNA.

However, these non-ERMS (particularly operational systems), which often make no proper provision for electronic record keeping, will continue to generate large quantities of valuable information for years to come.

**5.22 ERM in an NTFS (New Technology File System) environment**

*This is only a temporary measure and records should be exported into an ERMS as soon as it is available. If records are being held in NTFS and there are no plans to procure an ERMS, please contact Info-CMemERM for guidance.*

Records held in NTFS must be managed in such a way as to support their eventual migration into an ERMS.

If records are to be kept electronically in an NTFS file structure, they must be held in an environment that is as close to an ERMS as possible, using the capabilities of Windows Explorer.

The following principles apply when creating an NTFS document and record store:

- Identical NTFS file plans must be created according to the general guidance on file plans at Chapter 3. One of these will hold work in progress (WiP), the other will contain records.
- Users must be made aware that information (WiP and records) should only be stored at the lowest level (folder level) of the file plan.
- Each folder in the records area must contain a ‘ReadMe’ file with appropriate metadata, e.g. Name/role of folder owner, keywords, retention schedule.
- Access permissions must be established in the records file plan so that it is effectively made ‘read only’ to users. Users can therefore declare records (from the WiP area, Outlook etc), but cannot deliberately or accidentally modify or delete any records.

📎For certain types of record (e.g. contracts, deeds etc), it may be important to maintain an original paper copy. In these rare cases, IM staff must ensure that the record is held on a registered file, following the guidance for physical records set out in Chapter 3, and is linked to any related records held electronically.

📎If Units wish to keep records in an NTFS structure, prior authorisation must be granted by Info-CMemERM.

### 5.23 Migrating from NTFS file structure to an ERMS

Importing record collections from an unmanaged environment such as shared drives within Windows Explorer to an ERMS environment will impose a corporate information structure, with appropriate access controls and audit trails on those records. The main advantage of an ERMS is that once the records have been imported, the system will protect against their deletion, provide scope for additional metadata to be added, and impose strict rigours in regard to the management and hence the status of the imported record or collection of records. This then is supported by a full audit trail, which will document what actions were undertaken.

Electronic files held in a Windows Explorer environment may possess very little metadata compared with similar documents in an ERMS. Some new metadata may be added automatically by the importing ERMS but the manual addition of a full set of metadata to each document may not be feasible. Such documents may have to be imported with a minimal set of metadata. Users may be able to augment this metadata using additional metadata elements and tools available in the ERMS.

During bulk import of files from the Windows Explorer environment to an ERMS, there are two methods a Unit can consider:

g. Only those files in the Windows Explorer environment that have been deemed beforehand as being worthy of preservation may be transferred to the record management element of the ERMS. At this point, all the relevant metadata will be added to each record in turn. On completion of the import process, all documents remaining in the Windows Explorer environment should be destroyed.

h. For Units migrating to an ERMS with a document management capability, all files must be transferred as documents into folders with short retention periods. The SMEs can then select those documents worthy of retention by declaring them as records, whereupon they will acquire metadata establishing the appropriate retention periods and access privileges. Once the retention period of those ‘documents’ not declared as records takes effect, they can either be retained for a further short period, or destroyed.

If additional advice is required please contact Info-CMemERM.

### 5.24 Records stored outside of an NTFS environment must be managed in a way that supports their capture and preservation

IM staff managing information held on systems that do not have ERMS or use an NTFS file structure (e.g. operational systems Bowman, etc.) must contact Info-CMemERM to discuss the nature of the information held, and potential methods of record capture.

### 5.25 Electronic records must not be stored offline

Electronic records must not be maintained offline (e.g. on CDs, DVDs), as this makes them difficult for users to discover/access, and risks them becoming inaccessible due to media obsolescence.

No electronic records should be taken offline (even temporarily) without prior consultation with Info-CMemERM.

## Part C – Instructions for Project Teams introducing an Electronic Records Management System

### 5.26 General Principles

As most of the MOD will get ERMS capability when DII is rolled out, these instructions only apply to project teams introducing ERMS in areas that will **not** migrate to DII.

Staff responsible for the selection, configuration and implementation of ERMS in MOD must:

- Liaise with Info-CMemERM to ensure that ERMS and processes are consistent with Defence-wide policy and processes and that records management disciplines are maintained.
- Ensure that appropriate declaration, indexing and retrieval mechanisms exist for electronic records.
- Ensure that electronic records can be preserved.
- Ensure that the ERMS is designed and implemented to capture metadata about records to a level consistent with the MOD Metadata Standard (MMS), and that this is maintained over time.
- Ensure that actions carried out can be audited.

Any proposals for a new ERMS must be identified to and agreed by Info-CMemERM

### 5.27 An ERMS must facilitate the easy declaration and retrieval of records by users

Good ERM must be made as easy as possible, particularly at the record declaration stage. Ideally it should be easier to declare properly than not to declare at all, with as few mouse clicks as possible required to effect each transaction. The ERMS should be fully integrated with any Office Automation package in use so that it appears to be a natural extension of the package. For example, it should be possible to declare a record directly into the ERMS from within the word-processor, spreadsheet or mail facilities without the need for a separate 'file' transfer.

The mechanisms for the capture of records should ensure that:

- All types of record are captured.[6]
- Complete records are captured, e.g. an e-mail and its associated attachment, and associating these together in a meaningful and useful manner.

[6] ERMS should be able to handle all kinds of data object. However, there may be limitations on the storage of large and complex digital objects such as websites (e.g. all hyperlinks may not be stored) and active databases (ERMS may only store regular 'snapshots' of information)

The performance of the ERMS should not slow users down. Users should be able to quickly search with as few a mouse clicks as possible. Good industry standards in other respects such as scalability, maintainability, support, help facilities and documentation need also to be considered.

### 5.28 Records held in an ERMS must be fully searchable

All MOD records must be readily available to support business and operational needs, and to enable the Department to meet its statutory obligations under FOI, EIR, etc. Consequently, records must be searchable regardless of whether they are stored online in an ERMS, or elsewhere.

All ERMS have a range of in-built search capabilities and it is expected that they must have the following search functionality as a minimum:

- Support browsing and navigation of the file plan structure and allow selection, retrieval and display of electronic folders and their content through this mechanism.
- Be capable of full-text content searching.
- Be capable of creating and storing saved searches and making them available to all end users, including those users of other line of business applications.
- Allow the use of Boolean operands footnote of definition needed in the construction of a search.
- Present the search results as a list of folders or records. However it must also indicate to the user if the search yields no results.
- Not allow a user to have access to folders, records or their metadata, by means of the search and retrieval function, where the access controls and protective markings allocated to those folders or records are intended to prevent access by that user.
- Support the use of encyclopaedic lists (e.g. a drop down list of record types to search for).
- Allow a search on metadata field values.

### 5.29 An ERMS must capture appropriate metadata and maintain its links to the records

Metadata must be stored such that it is clearly and unambiguously attached to the record. Mechanisms within the ERMS must guarantee that metadata cannot become detached from the record content, or lost in some other way, and can always be transferred as a meaningful part of the record when migrating to a new system platform, or transferring into an approved format for permanent preservation.

In order for the user to enter metadata that will be both useable now and in the future, as many of the metadata elements as possible must be generated by the system, thus saving the user from having to enter large amounts of metadata for a record.

A MOD Metadata Standard (MMS) has been developed based on the e-Government Metadata Framework (e-GMF) that has been mandated for use throughout Government. The use of the MMS to establish appropriate metadata capture throughout MOD is a mandatory requirement on all ERMS implementations.

The minimum mandatory metadata elements that must be captured at the folder and folder part level are listed in the following table. These are taken from the e-GMS (e-Government Metadata Standard). It should be noted that some of this metadata will be inherited from the file plan metadata elements. The meaning and use of these metadata elements is defined below.

| | |
|---|---|
| Creator. Custodian | For documents originating outside of MOD, the person who has responsibility for the document within the MOD |
| Identifier. System ID | Unique reference number, automatically generated by system |
| Identifier. File plan ID | Identifier for a file plan object. Derived from the file plan itself e.g. DGInfo-4-1-1 |
| Title. Title | Meaningful name given to the object |
| Date. Opened | Date the folder/part was made available for records to be declared |
| Date. Closed | Date on which further additions were prevented |
| Relation. Is Part Of | Identifies instances where the content of a records has a direct relationship with that of another |
| Relation. Has Part | Identifies instances where the content of a record has a direct relationship with that of another or clarifies how one level of aggregation relates to other levels |
| Subject. Category | From the Defence Taxonomy |
| Subject. Keyword | From the Defence Thesaurus |
| Aggregation | Defines the required data at each level. System generated |
| Location. Home location [for physical formats] | Normal physical location of the object/information |
| Location. Current location [for physical formats] | Current physical location of the object/information. Enables tracking [user generated] |

| | |
|---|---|
| Security. UK Protective Marking | Allows automation of restrictions and permissions to view records e.g. RESTRICTED |
| Security. National caveats | Additional protection for protectively marked material e.g. UK EYES ONLY |
| Security. Descriptors | Identifies the nature of the sensitive information e.g. SECRET-MANAGEMENT |
| Security. Username access lists | A list of all those allowed access to the resource |
| Security. Business group access permission | Group(s) to which access to the information is limited, e.g. PERSONNEL – All personnel mgrs |
| Rights. FOI disclosability indicator | Mandatory at folder, part & record level |
| Rights. FOI exempt | Information falls within scope of one of the absolute exemptions under the FOI Act |
| Rights. FOI released | Information published, or due to be published, under the Publication Scheme. |
| Disposal. Disposal Schedule ID | Unique identifier of disposal schedule applied e.g. D5 |
| Disposal. Disposal action | Action to be taken when disposal condition is reached, i.e. destroy, review or export |
| Disposal. Disposal time period | Identifies when disposal action is to be taken, e.g. D5 |
| Disposal. Disposal event | The event that may trigger the disposal action, e.g. upon closure of file part |
| Disposal. Disposal (due/effective) date | Date when action will be triggered e.g. If ‘D5’ – 5 yrs from file part closure |
| Disposal. Disposal authorised by | Name/role of individual who authorised disposal |
| Disposal. Export destination | If exported, the destination of the information |

### 5.30 Record Level Metadata

The additional minimum mandatory metadata that must be captured at the record level is listed in the table below.  As much of this metadata as possible should be inherited from the upper levels or generated by the system.

| | |
|---|---|
| Creator. Creator | The person, post, team or organisation responsible for the content of the resource (or the person who caused the resource to be brought into the business unit), up to the point of declaration as a record. |
| Date. Created | Date (and time [optional]) the resource was created. System generated. |
| Date. Acquired | Mandatory for e-mail, optional for other records but recommended for all externally produced material. System generated. |
| Date. Declared | Date (and time [optional]) a document of business activity was declared to be a formal record. System generated. |
| Addressee. To | The person (or persons) to whom the record was addressed. |
| Type. Document type | Type of record that in some respect displays different behaviour from that expected in the default type. |
| Relation. Copy [/Pointer] | Identifies instances where the content of a record has a direct relationship with that of another or clarifies how one level of aggregation relates to other levels. System generated. |
| Relation. Redaction/Extract | System generated. |
| Relation. Reason for Redaction/Extract | User generated. |
| Relation. Rendition | System generated. |
| Rights. Disclosability to DPA data subject | User generated, Y/N (default = N) |
| Rights. EIR disclosability indicator | User generated, Y/N (default = N) |
| Disposal. External event occurrence | The external event that may trigger the disposal action. |

In order to make best use of the ERMS ability to track the physical location of items and schedule their review for destruction or further preservation, an appropriate record type (and associated metadata that should include the ‘location’ element) must be created.

The MMS in not intended to be a comprehensive list of metadata items to be used in the MOD, and the list of potential metadata elements is almost limitless. Therefore before adopting any optional metadata elements, reference must be made to the Defence Data Repository (DDR) to ensure compliance with JSP 329 – Data Management Policy. The following are examples of additional metadata fields that may be applied to meet more specific business requirements:

- Addressee post
- Addressee business unit
- UK Military service staff number
- UK MOD Civil service staff number
- Contract number
- Drawing number
- Map reference code

**5.31 The system must be able to grant and/or restrict access to records in order to meet business, security and legal requirements**

The key characteristics of an effective approach to managing the security and access of records are:

- Authentication: assurance of the identity of a user, that users are in fact who they claim to be and that they are the true originators of records to which their names are attached.
- Access control: that a particular user is sanctioned for a particular function, for example, to be able to create a new version of a record, or to alter the filing or retention decisions pertaining to a group of records.
- Confidentiality: ensuring that content access is granted only to those who should have it.
- Integrity: evidence that the contents of the record, including metadata and format, have not been altered since the document was declared as a record, as a result of control procedures which would prevent this.
- Non-repudiation of transmission: protection against denial by an individual originating a communication that is stored as a record, as a consequence of assurance gained from the previous four characteristics.
- Non-repudiation of receipt: protection against denial by an individual in receipt of a record.

It must not be possible to edit the contents of a record without creating a new version. Similarly, delete rights (for records, rather than documents) should only be available to the ERMS administrators.

It is unlikely that ERMS will be implemented in isolation from other information systems. These systems will make use of existing security services and must follow existing System Security Policies (SSP), and any ERMS implemented will need to operate within that SSP.  Project staff should contact their security authority for advice.

### 5.32 An ERMS contains a series of pre-defined retention schedules

Users/IM staff must not be able to create their own retention schedules within the ERMS. IM staff should be able to select an appropriate retention schedule and apply it to a class/folder as necessary.

The retention schedules recommended for ERMS implementation by Info-CMemERM are:

- 02 years from date of closure.
- 05 years from date of closure.
- 07 years from date of closure.
- 10 years from date of closure.
- 25 years from date of closure.

If there is a perceived need to alter/diverge from these retention schedules, please contact Info-CMemERM for guidance.

A two month disposal retention schedule is also available.  This schedule must only be applied to 'DeleteMe' style folders that have been created to contain folder parts that have been created in error or for duplicate documents which may have been filed by mistake.

### 5.33 ERMS and any actions performed within them must be fully auditable

Audits are required for statutory reasons and as part of a Unit's corporate control procedures, especially in those areas where there is a strong requirement for authenticity.

Proper audit requires that all operations performed and procedures used to achieve long term preservation of electronic records are clearly defined. Responsibility for undertaking theses actions must be appropriately assigned.

To remain an authentic representation of events, a record should not be capable of being changed. Since electronic information is more vulnerable to accidental or deliberate editing, without leaving any traceable evidence within in its own content, the ERMS must take special measures to prevent retrospective change to records and to capture other significant actions taken on them.

The degree to which the authenticity of a record can be demonstrated for legal and accountability purposes will be largely determined by the success of these restrictions.  Where it may be necessary to gain update/amend access to maintain the record, to edit the metadata, and take any other action that will modify an attribute of the record, pre-determined procedures and roles should defined, fully documented and adhered to.

New and related versions of the record can be created by making and editing a copy, and saving this as a new record; for example, it may be appropriate to retain various versions of a document as it passes through draft to finalisation. The ERMS should be capable of linking together versions of the same record, either automatically by the system or through the use of strict naming conventions, to ensure that the latest version is retrieved by a user search. The user should be aware that earlier versions of the record exist in the system.

Although it is possible for ERMS to track all activities relating to the record, including all read and retrieval access, it may not be sensible to do so in all cases. The IM staff and systems administrators should give careful thought to the extent that this information will be useful and the long-term use that will be made of accumulating such detailed data.  It may be appropriate to restrict this full auditing functionality only to certain categories of record, or to certain groups of users. The more the audit log records, the more it costs in processing overhead.  It would therefore be wise to capture the bare minimum events such as record capture, record review, any security breaches and destruction.

Audit activities should be triggered by particular events or on the transfer of records. The information that needs to be gathered and checked against specified criteria will include:

- The process being audited.
- The records being processed.
- The date and time of the event.
- The person responsible for the event.
- Any other relevant comments.
- The transmission and receipt logs.

Audit trails should be provided for all records.  Audit trails should be kept securely, and are available for inspection by authorised internal and external personnel. The audit trails should be capable of being easily followed by auditors who may not have experience of the technologies in use.

### 5.34. Electronic records stored in ERMS must be managed in such a way as to demonstrate their evidential weight.

The Civil Evidence Act (1995) does not specify any special conditions governing the use of computer-derived evidence in court. However, in criminal proceedings, Section 69 of the Police and Criminal Evidence Act 1984 states that any statement produced by a computer will only be admitted into court subject to compliance with certain conditions. One of these conditions provides that "at all material times the computer was operating properly".

An ERMS should, as far as possible, seek to conform to the provisions of BIP 0008-1:2004 - A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. The level of authenticity of an electronic record is significant if the MOD ever needs to use the record in legal disputes. Compliance with BIP 0008 cannot assure evidential worth - ultimately this is for the courts to decide – however, non-compliance provides no mechanism to support arguments for evidential worth and without such mechanisms it will be difficult to satisfy the needs of audit. Issues to bear in mind include:

- Are the records complete?
- Are they accurate?
- Are they valid?

The Compliance Workbook for Legal Admissibility of Information Stored on Document Management Systems, BIP 0009 is designed to establish the compliance of a document management system with BIP 0008. It also enables an audit trail of compliance to be produced that must be stored on the records management application as a record held on the system. When completed, this workbook is the owning organisation's statement of the extent to which its ERMS and the records within it comply with the recommendations in BIP 0008.

### 5.35 Electronic records must be held in a suitable format to aid retrieval and further use

The formats currently available that meet the requirements defined for transfer, either for export or migration purposes, are PostScript, TIFF, SGML, PDF and delimited file formats (such as comma separated variable). Each of these formats is appropriate for specific record types described in more detailed in the following paragraphs. These transfer formats are robust and are considered to have a long life ahead of them, however conversions should be kept to a minimum because any format conversion is likely to incur some data loss.

- Postscript - Any application designed to run on a desktop computer will support Postscript printing.  Since Postscript is designed to be written to file as well as to a printer, it can be used for electronic record transfer.
- Portable Document Format (PDF) – is a variety of Postscript and is a universal file format that preserves all the fonts, formatting, graphics, and colour of any source document, regardless of the application and platform used to create it.
- Tagged Image File Format (TIFF) – is one of the most popular and flexible of the current public domain raster file formats.  The main strength of TIFF is that it is a highly flexible and platform-independent format that is supported by numerous image-processing applications.

- Comma Separated Variable (or Value) (CSV) – is a way to collect the data from any table so that it can be conveyed as input to another table-oriented application. It contains the values in a table as a series of ASCII text lines organized so that a comma from the next column's value separates each column value and each row starts a new line. This format is suitable for spreadsheets and small databases.
- Standard Generalised Mark-up Language (SGML) – is a formal language that can be used to pass information about the component parts of a document to another computer system. Web pages are typically encoded with a set of tags called Hypertext Mark-up Language, (HTML); SGML is the parent language, the tag-set building rules, for HTML and for most other descriptive tag-sets.

To comply with the requirements of the e-Government Interoperability Framework (e-GIF) standard, adoption of Extensible Mark-up Language (XML) as the primary standard for data integration is mandated. XML is the universal format for structured documents and data on the Web. XML is a restricted form of SGML that enables the definition, transmission, validation, and interpretation of data between applications and between organizations.

Metadata describing folder structures, contents and relationships between objects stored in the ERMS should be transferred with the records, so that the metadata and the links to the record are not broken. The metadata should comply with the minimum mandated in the MMS.

**5.36 All records held within an ERMS must be protected from modification, deletion, or loss.**

By definition an ERMS should preserve the records held and prevent their accidental or deliberate modification or deletion.

A preservation strategy must exist which addresses the potential loss of electronic records due to:

- The obsolescence of the applications format so that the content cannot be read.
- Media obsolescence or deterioration.
- Changes to the structure of the Unit that creates and manages the records and gives them context

In addressing these concerns, the following must be considered:

- Maintain and preserve or emulate the original application programmes in which the records were created and held. Where the original application is to be used, it is imperative that the Unit makes provision for an annual review of all applications and platforms to ensure that appropriate support is given for all originating technology. This option is only viable however for the short to medium term. MOD's preservation strategy insists upon a longer-term preservation, i.e. for periods of seven years and longer.

- Provide a migration strategy where it will be necessary to ensure that any change to another platform takes account of both the migration requirements of records held in native formats and the requirement to preserve the integrity of the information, i.e. electronic records should be stored together with the contextual metadata in a stable area of the business unit's workspace to ensure they cannot be modified or deleted by users.
- Ensure that, as far as possible, the electronic file plan is based on functions/outputs, rather than organisational structure. This should guard against the effects of organisational change.

If records are to be preserved in a usable form, consideration needs to be given to the metadata that is required to ensure continued accessibility and to demonstrate the authenticity and integrity that confers their status as corporate records. In the absence of audit trails, for example, authorship may be unclear and it will be difficult to ascertain the business context of a document. Preservation of documents without their contextual metadata will compromise any preservation strategy.

**5.37 An ERMS must be able to support the transfer of records between systems**

Once an ERMS has been adopted, it may be necessary to transfer a folder containing records or a series of folders to another ERMS.

An electronic record is the sum of the record, its context, metadata and the audit trail to establish provenance. Contextual information and metadata must remain linked to the record. The ERMS export mechanism must:

- Treat the record as an entity, including context, metadata and audit trail information.
- Must be able to export a record at any point in its lifecycle.
- Ensure no loss of information.
- Enable the audit trail to be annotated with any changes.
- Facilitate the physical transfer of the records.

Records that are held in the ERMS for many years may also need to be migrated to a new system in their entirety in order to ensure their ongoing preservation. Migration is the transfer of the contents of an entire file plan, from one hardware and software environment to another. The objective is to preserve the integrity of the records and to ensure they can be retrieved and viewed in the future.

It is therefore extremely important that the ERMS has a capability to export, and by implication import information to and from other ERMS environments.

Records should always be verified when written to new formats, migrated or copied for refresh or backup purposes, and special note made of any loss of data.

Two backup copies should also be stored separately from the working versions, preferably off-line with one off-site. This should guard against catastrophic events, as well as migration issues. If new copies are required, the master should always be returned to the secure store dedicated for its use.

# Chapter 5 - Annex A

## MOD Policy on Digital Storage Media

## Introduction

*This policy is mainly concerned with information stored on media for preservation purposes in an off-line archive. Such use of off-line media must be regarded as exceptional and Corporate Memory must be consulted for approval and advice in all cases.*

Digital information must normally be stored in on-line server-based hard disk storage wherever possible. Such storage affords the best levels of security, accessibility and search capability. Server-based data is generally well managed and backed-up and would normally be migrated to new storage during system upgrade. Information held only on off-line storage is much less available for use and is generally more vulnerable to loss due to damage, deterioration and simple misplacement of the media or technology obsolescence.

However, it is recognised that there are occasions when writing information to off-line media constitutes a cheap and easy solution when on-line capacity is exceeded or when it is necessary to transfer data to another system.

### Reasons for Storing Information Off-line

There are essentially three reasons for writing information to off-line media:

- Transfer of information (to another system)
- Short-term security (e.g. as a back-up to recover from system failures). Normally the media used for purposes such as back-up are re-cycled so that they are over-written periodically (e.g. monthly).
- Preservation (as an off-line archive) i.e. record keeping.

NB. Off-line media should only be used for record keeping purposes after obtaining approval from Corporate Memory.

### Storage Requirements

There are several storage requirements which affect the choice of media for a particular application. These requirements are likely to include:

- Capacity – the media must have sufficient capacity compared to the volume of information to be stored so that as few items of media as possible are used. Large numbers of media will have a major impact on retrieval time, if only specific information is required, especially if the media has to be individually loaded manually - as is likely to be the case unless some form of multi-disk changer or ‘juke-box’ is used. A factor to be taken into account when estimating required capacity is that the average size of electronic files is increasing as new generations of software are introduced (e.g. typical MS Word documents are becoming larger for the same amount of text content with every new version of Word released).

- Random versus Serial access – some media are inherently serial in nature (e.g. magnetic tape) whereas some are random (e.g. CD ROM). Serial access may be ideal for system back-up purposes but is probably not practical for archive purposes where it is likely that only selected records will be required from the many thousands stored on a single item of media.
- Longevity – the media must be viable for reasonable periods (normally ten years) under normal conditions. However, longevity beyond this period may be of no benefit if the technology to read the media becomes obsolete in the meantime.
- Obsolescence – computer storage media become obsolete over relatively short periods (e.g. 10 years or less). Information stored on media will need to be refreshed to new media roughly every ten years (at least), judging by the current rate of development.
- Cost – off-line media may appear to be very cheap compared with additional server-based disk capacity but the cost of additional hardware and software, storage equipment and staff to manage the off-line media library must also be taken into account when comparing different media types.
- Susceptibility to damage - storage media may need to be physically robust especially if it is likely to be read and re-used many times. Some media like removable hard disk drives may be easily damaged by shock (i.e. Dropping onto hard surfaces) or by frequently plugging and unplugging connectors. Also some media may be seriously affected by environmental conditions such as heat, humidity, sunlight and magnetic fields.

### Back-up Copies

All forms of media can develop faults or be damaged or lost. It is essential to hold two copies of each item of media to guard against mishaps. The two copies should be held in different locations to guard against the same mishap affecting both copies.

### Index of Contents

Where off-line media are used for record keeping purposes it is essential to maintain an external index of the contents to facilitate searching and review. Without such an index the only way to discover the contents is to load each item of media individually. For convenience the external index may be held in electronic form, such as a spreadsheet, or printed onto paper, a copy of which must be held with the media collection.

## Choice of Storage Media

The following paragraphs identify the main characteristics of a range of common storage media affecting the choice of media for different purposes. The main factors in making a choice are tabulated in a decision table at the Appendix to this Annex.

### On-Line Server-Based Hard Disk

This is the best choice for record keeping purposes because it affords the best levels of security, accessibility and search-ability. Server-based data is generally well managed and backed-up and is normally protected against unauthorised access by system permissions. Because it is nearly permanently on-line it can be made widely accessible, even world-wide if necessary. Server-based information would normally be migrated to new storage and may even be converted to new data formats during system upgrade thus overcoming the obsolescence issue. This is not an option for either information transfer or short-term security purposes which both require that information be held on removable media.

### CD ROM and DVD

Compact Disks (CD) and Digital Versatile Disks (DVD) are generally a good choice for storing relatively small volumes of data (i.e. A few Gigabytes) for periods up to 10 years. Only Recordable versions of these media (CD-R and CD+R, DVD-ROM) should be used to avoid the risk of inadvertently over-writing valuable information. Re-writeable versions (CD-RW and DVD-RW) should not be used. Tests have shown that the so-called ‘Gold’ disks which use gold as the reflecting layer within the disk have a long life and are suitable for preservation purposes. It should be noted that the data retention properties of optical media deteriorate rapidly if not kept in an acceptable environment (i.e. a normal air-conditioned office environment, out of direct sunlight and UV light). See Reference C below for more information.

### Floppy Diskette

Floppy disks, although still readily available, are not considered a viable storage medium as they hold only about 1.3Mb, are easily overwritten and the recording surface can be easily damaged. This medium is likely to become obsolete within a few years. Reliable life-expectancy is about 5 years only. Floppy disks should only be used for the transfer of small files between systems and not for preservation purposes.

### Removable Hard Disk

Removable hard disks are available in capacities up to 100Gb and greater. This medium may be preferable to CD ROM or DVD for the storage of many Gigabytes of data - if it is necessary to search all of the data simultaneously - and for the convenience of accounting for much fewer items of media. The drawback of removable hard disks is that a single fault to a disk or drive could render all the data inaccessible. For this reason it is essential to hold two disks with identical copies of the data, one as a back-up in case the primary disk fails.

### Magnetic Tape Cartridges

Digital Audio Tape (DAT) and Digital Linear Tape (DLT) are media most commonly used for system back-up purposes where the lack of a random access capability presents no problem. Storage capacity is high (100Gb and more). Generally this type of media is unsuitable for records purposes.

## Mass Storage Devices

Mass Storage Devices usually make use of large numbers of magnetic media (such as those described above) to store many Terabytes of data. The individual media are loaded robotically sometimes in ‘jukebox’ fashion. These devices are an extension of on-line storage architecture and usually have to be built into the overall architecture during system design.

### Memory Sticks and other ‘Flash’ Memory Devices

Flash memory devices are extremely compact. They have rather low capacity (up to a few Gigabytes) and to date do not have a long enough history of use to determine their likely longevity. Consequently they are not considered suitable for records purposes but are an excellent transfer medium. For security reasons the use of memory sticks may be forbidden on networked systems. Users must check their own system’s Security Operating Procedures before using such devices (See Reference D below [Part 8, Section 3] for policy and guidance on security).

### Paper and Microform

Paper and microform are not digital storage media but may still be considered as a means of storing information which has been generated electronically even though the general trend is towards preservation in electronic formats. Both paper and microform offer reliable long term preservation using well established methods and equipment. Paper may be a suitable medium where there is already a large collection of records on a topic to which the new electronic records could be printed off and added. Transfer to microform could be an option for reliable long term preservation where the space to keep large volumes of paper records is not available.

## Information Assurance

Media holding archived data must be actively managed. They should be regularly checked to ensure their availability (i.e. they still exist and can be readily found) and that they have not suffered physical degradation. Media must be replaced as required to ensure that information remains available.

## Related MOD Policy

The Security aspects of the management of digital media (marking, control, handling and erasure) are covered in JSP 440 Part 8, Section 3, Chapter 2, ‘Media Management’. The standards of JSP 440 should be adhered to for all media.

## Further Advice and Guidance

Further advice and guidance on the use of Digital Storage Media is available from The National Archives web site (See References A and B below) or from Info-CMemERM staff.

## References

a. TNA Digital Preservation Guidance Note No 2 – Selecting Storage Media for Long-term Preservation

b. TNA Digital Preservation Guidance Note No 3 –Care, Handling and Storage of Removable Media

c. JRNIST Stability Study

d. JSP440 – MOD Manual of Security

# Chapter 5 - Annex A - Appendix 1

## Choice of Storage Media – Decision Table

| | System-to-System Transfer | Short-term Security | Record Keeping |
|---|---|---|---|
| **On-line storage** | Not an option. | Not an option. | Best option. Offers security, accessibility and some future-proofing. |
| **CD ROM and DVD** | Possible option for volumes up to a few Gigabytes. | Possible option for volumes up to a few Gigabytes but not reliable for frequent re-use of media. | Not recommended for record keeping purposes, however in highly exceptional circumstances a possible option for volumes up to a few Gigabytes for periods up to 10 years.<br>Must be approved by Info-CMemERM. |
| **Floppy Diskette** | Possible option for transfer of small files. | Not an option. | Not an option. |
| **Removable Hard Disk** | Best option for transfer of volumes more than a few Gigabytes. | Possible option, but consider the implications of frequently plugging/unplugging the device. | Possible option for volumes greater than a few Gigabytes for periods up to 10 years.<br>Must be approved by Info-CMemERM. |
| **Magnetic Tape Cartridges** | Possible option where the same format of tape can be used on both the source and target systems. | Best option for system back-up purposes. | Not an option for normal records purposes. |
| **Mass Storage Devices** | Not an option. | Not an option. | Possible option for making a major increase to the capacity of an on-line system. |
| **Flash Memory Devices** | Possible option for volumes up to a few Gigabytes. | Possible option for volumes up to a few Gigabytes but comparatively expensive. | Not an option. Unproven longevity and expensive for records purposes. |
| **Paper and Microform** | Not an option. | Not an option. | Possible option especially where paper/microform records already exist. |

# Chapter 6

## Film, Video and Photographs

### 6.1 Film and Video Records

Films/videos may range from full productions, such as public relations and training films, to records of tests, trials, operations, reconnaissance etc. They may be edited or unedited and of any duration. They may or may not bear a protective marking.

Each year, any business unit responsible for making or sponsoring a film/video in the preceding year is to forward details to Info-CMemR, who will, in turn, liaise with The National Archives to identify films which appear to warrant permanent preservation. Selected films/videos will be transferred to the Imperial War Museum (IWM) - (for subjects primarily of military interest) or the National Film and Television Archive (NFTA) - (for other subjects).

The process for packaging and sending material of this nature to Info-CMemR and for onward dispatch to a pre-approved location can be found at Chapter 7, Annex B and must be followed.

### 6.2 When to Transfer Film or Video Records

Selected master copies should be forwarded to the IWM or NFTA as soon as possible after their selection has been confirmed by Info-CMemR and not later than 10 years after their creation. Info-CMemR will confirm the appropriate recipient of selected material.

### 6.3 What Should be Transferred?

In the case of film, a master copy will be either the original negative or a good quality duplicate negative, fine grain positive etc. In the case of video, a master copy will be either the original tape or a broadcast standard duplicate. A viewing copy of the film should be transferred with the master. When a film is produced in different versions it is important to forward both a master and viewing copy of each version.

Film transferred must be accompanied by any documents relating to its production e.g. scripts, shortlist etc. as well as posters and training notes.

### 6.4 Films or Videos which Do Not Merit Preservation

Films and / or videos not required for preservation are to be destroyed when they are no longer needed for official purposes. Info-CMemR must be advised in writing of any case in which the material is still required by the business unit 25 years after its creation.

### 6.5 Warning Concerning Films pre-dating 1952

Any business unit retaining 35mm film appearing to date from 1952 or earlier should isolate the film and, as a matter of urgency, contact the Film Department of the Imperial War Museum (020 7416 5289) for advice. Such film is likely to have been printed on cellulose nitrate stock and constitute a very serious fire hazard.

### 6.6 Still Photographs and Microfilm

Each MOD business unit holding still photographs and microfilm is responsible for deciding whether they are of sufficient historical interest to merit permanent preservation. To assist in this task, the following guidelines should be used (refer also to Chapter 7, Annex A):

- Age of material - Material should normally be retained for 5 years before they are considered;
- Quantity - Only a small selection of the annual output should be transferred. As a rule, no more than 200 photographs;
- Subject matter - Subjects likely to warrant preservation include exercises, new equipment, senior personnel or material related to a major incident;
- What to transfer - Both a negative and a print should be forwarded. Both colour and black and white is acceptable. All material should be accompanied by some kind of supporting documentation.

**NOTE:** These instructions do not apply to photographs or micro films which form an integral part of a registered file. Such photographs are not to be removed from the file which is to be reviewed in the normal way.

### 6.7 Photographs which Do Not Merit Preservation

Photographs which do not merit permanent preservation should be destroyed when they are no longer needed for official purposes. Info-CMemR must be advised in writing of any case in which the material is still required by the business unit 25 years after its creation.

### 6.8 Where to send Photographs

Photographs selected for preservation should be forwarded to the Imperial War Museum after contact has been made to arrange the transfer. The contact point is:

- The Keeper
  Department of Photographs
  Imperial War Museum
  Lambeth Road
  London SE21 6HZ
- Tel: 020 7416 5000

### 6.9 Service Museums

If, exceptionally, it is felt that surplus film, video or photographs not worthy of preservation by the Imperial War Museum may, nevertheless, be of value to a Service museum full written details of the nature of the material concerned must be forwarded to Info-CMemR. If appropriate, Info-CMemR will seek approval from the Lord Chancellor for the "presentation" of the material to the relevant museum.

# Chapter 6 - Annex A

## Microform Records

b. The term microform includes microfilm, microfiche and other similar formats, such as aperture cards, jacketed fiche and blipped film.

c. As far as possible microform records should be passed to Info-CMemR in the original negative form along with a silver nitrate copy and should conform to BS 5699.

d. The following storage conditions are recommended:

   - temperature 16C to 2OC
   - relative humidity - Acetate 15 to 40%
     - Polyester 30 to 40%

   Rapid changes in environmental conditions should be avoided.

e. There may be occasions when only part of a microfilm or microfiche might be worthy of permanent preservation (for example, where a microfilm consists of copies of a number of registered files). In those circumstances, however, the whole film or fiche should be forwarded with a covering note identifying the files which are recommended for permanent preservation.

f. To enable individual documents to be identified, each microfilm and microfiche must have some indication of its contents and each frame must be numbered (foliated).

g. Contents are most conveniently indicated by a title frame at the beginning of each film or part of a film and at the first frame of a fiche (top left hand corner) and this should be carried out as normal practice during initial filming operations.

h. If you require further advice regarding microform records please contact Info-CMemR.

# Chapter 6 - Annex B

## Disposal Arrangements – MOD Security - Sensitive Image Records selected for Preservation

Within the scope of the Public Records Act 1958, material may be selected for preservation either as deposited records under Section 4(1) of the Act, or as records to be presented under Section 3(6).

MOD's policy is that imagery selection should occur five years after creation. The result of this process is normally that video*/photographs, of a military nature, selected for the national archive are deposited at the Imperial War Museum, while those of more limited or predominantly local interest may be presented to an appropriate institution.

*[**NOTE:** the term "video" is used to describe moving film in both cine and video-cassette format]*

Records selected for preservation but which still merit a security protective marking cannot normally be transferred to the place of deposit/presentation until the need for that marking ceases.

**1. Procedure for video/photographs, still sensitive, selected for deposit or presentation**

a. Material must be packaged within boxes of archival standard.

b. Within the box, photographs (whether negative or print) must be individually enclosed within photographic envelopes, each envelope marked with an identifying number or text.

c. Individual videos must be marked likewise, on the video-sleeve/box and also on the video cassette/cine-reel itself.

d. Within each archive box must be placed a consignment instruction giving the following:

   – a hardcopy list identifying the contents by subject (also by serial number if appropriate)

   – the review decision for each item (i.e. deposit or presentation)

   – the institution selected to receive it

   – the recommended year of its next sensitivity review - no more than 10 years ahead

   – a brief explanation of its current sensitivity

   – signature, name and position of reviewing officer, and the date

e. The archive box must be marked externally with the following:

   – "Image records for sensitivity re-review"

   – the source of the imagery (e.g. "DSTL Porton Down")

   – the earliest recommended review year on the consignment instruction

  - the highest protective marking applicable to the contents

f. A second copy of the consignment instruction must accompany the archive box.

g. The archive box must be sent, in accordance with appropriate JSP 440 procedures, to:

  - Info-CMemR

    Ministry of Defence
    06.G.01 Main Building
    Whitehall
    London SW1A 2HB

**2. Conflict between business use and archival preservation**

Usually, business use of image records has lapsed after five years. If it has not and the video/photograph is selected for preservation, a copy must be created. The copy will be retained locally, clearly marked "Copy - destroy when business value ceases; original has been selected for preservation at <name of chosen institution>". The original will be despatched following the above procedures.

# Chapter 7

## Forwarding Material to DG Information - Corporate Memory Records

### 7.1 When to Forward Records to - Corporate Memory Records (Info-CMemR)

Records held by MOD HQ and other civilian business units should normally be forwarded to the relevant archives within 5 years of their closure unless the business unit has identified an ongoing administrative need to retain the records locally. Where this is the case the records may be retained for an extended period however they must be forwarded to Info-CMemR within 25 years of their closure unless prior written authority has been obtained from Deputy Director Info-Corporate Memory to retain them.

Records held by Service HQs, formations and units may be retained locally for up to 25 years after their closure though they may be forwarded to Info-CMemR at any time in the intervening period if they have ceased to have administrative value but merit consideration for permanent preservation. Info-CMemR should also be contacted before unregistered records are forwarded, unless they form part of a "rolling" arrangement. No records should be retained for longer than 25 years without the written approval of Deputy Director Info-Corporate Memory.

If you plan to send a large quantity of records to the relevant archives please contact Info-CMemR first to appraise of the type and quantity of records involved. This will ensure that suitable provision can be made for their arrival.

### 7.2 Closure of Business Units

When a branch is due to be closed (or a ship decommissioned) the administrative authority must include detailed instructions which make provision for the appropriate disposal of the records held by that branch. If records are to be transferred to another branch action should be taken as detailed in this JSP. Records which are not to be transferred to another business unit but nonetheless appear to warrant permanent preservation, or to have long term administrative value, should be forwarded to the administrative authority for appropriate action. Where this is not practical advice should be sought from Info-CMemR.

All business units are required, as part of their planning process, to make funding provision for movement and archive of records. As part of this process, Info-CMemCMT is to be notified. Info-CMemCMT will provide assistance with planning and costing of movement of records that are destined for TNT Archive Services in accordance with paragraph 8.5 below.

### 7.3 Machinery of Government Change

All business units liable to be affected by a Machinery of Government (MoG) change should carry out advanced planning so that transfer of records, information and knowledge can be achieved both smoothly and quickly.

Business units affected by a MoG change must have a clear understanding of their roles and responsibilities and will need to work closely with Info-CMemR to achieve an effective transfer of their paper and electronic records, as well as informally held information and knowledge.

Broad guidance on the transfer of records, information and knowledge as a result of a MoG change, can be found on the Defence Intranet or by consulting with Info-CMemR. This guidance is also useful for those personnel who are involved in preparing their business units for closure.

### 7.4 Scientific and Technical Reports

Business units which create or sponsor scientific and technical reports and similar documents should include Info-CMemR on the distribution list when the reports are issued. They will be retained and, at a later date, considered for permanent preservation. They will be held in secure conditions and only the originating business unit will have access to them.

### 7.5 Transfer of Records to The National Archives

Records which are identified as worthy of permanent preservation are then prepared for transfer to TNA: assigning them to an appropriate TNA "class" (the term used by the TNA to categorise different types of record) and allocating an individual reference number. Records are then normally transferred to TNA and generally made available immediately after transfer. The TNA Catalogue is available to view on the internet at www.nationalarchives.gov.uk.

The Public Records Act makes provision for the continued closure of some records which are identified as being too sensitive to release after 30 years. This may be on the grounds of national security or personal sensitivity. Such records can remain closed for an extended period, either held by TNA or retained by MOD. However, the Lord Chancellor's approval must be sought and it is therefore imperative that records which might warrant continued closure are identified to Info-CMemR within 25 years of their creation/closure. Any business unit holding records in this category should write to Deputy Director Info-Corporate Memory who will provide specific guidance.

### 7.6 Sending Records to DG Info-Corporate Memory Records

There is more than one destination for records being forwarded to Info-CMemR. The appropriate destination is determined by the type of record involved. Listed below are details of the different types of records generated by business units and the appropriate place to send them:

| Originator | Type of Record | Send to: |
|---|---|---|
| All | Registered files (other than TOP SECRET and Codeword and files containing Atomic and Nuclear records).<br>Further guidance can be found at ANNEX B to Chapter 7. | TNT Archive Services<br>Tetron Point<br>William Nadin Way<br>Swadlincote<br>Derbyshire, DE11 0BB<br>Tel: 0800 100600<br>Fax: +44 1827 301301<br>www.tnt.com |
| All | TOP SECRET and Codeword files and records.<br>Further guidance can be found at ANNEX A to Chapter 7. | Sensitive Archive<br>Room 012<br>Old War Office<br>Whitehall<br>London SW1A 2EU<br>Tel: 9621 78496<br>(020 7807 8496) |
| All | Atomic and Nuclear records. | Sensitive Archive<br>Room 012<br>Old War Office<br>Whitehall<br>London SW1A 2EU<br>Tel: 9621 78496<br>(020 7807 8496) |
| All | Civilian personnel records. | TNT Archive Services<br>Tetron Point<br>William Nadin Way<br>Swadlincote<br>Derbyshire, DE11 0BB<br>Tel: 0800 100600<br>Fax: +44 1827 301301<br>www.tnt.com |

| Originator | Type of Record | Send to: |
|---|---|---|
| All | All other records. | TNT Archive Services<br>Tetron Point<br>William Nadin Way<br>Swadlincote<br>Derbyshire, DE11 0BB<br>Tel: 0800 100600<br>Fax: +44 1827 301301<br>www.tnt.com |
| Certain Air Force Department Files<br>(See Chapter 4, Paragraph 4.1) | TOP SECRET, Codeword and Atomic. | AHB1 (RAF)<br>266/U4<br>RAF Bentley Priory<br>Stanmore<br>Middx, HA7 3HH<br>Tel: 7825 BP<br>(020 838 7000 x 7825) |
| As above | Other Air Force Department files. | AHB4 (RAF)<br>266/G4<br>RAF Bentley Priory<br>Stanmore<br>Middx, HA7 3HH<br>Tel: 7315 BP<br>(020 838 7000 x 7315) |

### 7.7 Retrieval of Records from DG Info - Corporate Memory Records

If there is a need to consult records which have been submitted to Info-CMemR, originating business units can request their temporary return by contacting Info-CMemR1. In the case of records held at Swadlincote an Asset Request Form should be forwarded to TNT. In the case of records held by the Info-CMemR Sensitive Archives, requisitions should be sent to Info-CMemR.

Closed records recovered from the archives must not be added to or altered in any way and must be returned to the archives as soon as they are no longer required.

Guidance for using the Archives at Swadlincote and the Info-CMemR Sensitive Archives can be found at Chapter 7, Annexes A and B.

### 7.8 Sending Unregistered Records to DG Info - Corporate Memory Records

Unregistered records (e.g. records not on registered files) might include maps, plans, drawings, and charts. Such records should be reviewed in the same way as registered files to determine whether they merit consideration by Info-CMemR for permanent preservation. Where they merit such consideration they should be forwarded as outlined below.

Such records should, wherever possible, be placed in standard archive boxes, though bound volumes may be sent unboxed. Each box or package is to be accompanied by a list of its contents, in duplicate. The highest classification of the enclosed material, the year of its origin and the reason that its permanent preservation is being recommended must also be indicated.

# Chapter 7 - Annex A

## Forwarding Material to the Ministry of Defence Corporate Memory Sensitive Archives

### 1. General Guidance

Staff should telephone or fax the MOD Sensitive Archives before dispatching more than 2 sacks of files, or other records e.g. books or ledgers, to advise on the amount of material for receipt. Agreement can then be reached regarding the quantity, manner and size of packaging, and timescale for the dispatch of material **(SACKS ARE TO WEIGH NO MORE THAN 11kg (24.2lbs))**.

Branches must keep a record of ALL material sent to the archive including the date of dispatch.

### 2. Registered Files

Each file must contain a completed MOD Form 262F showing the disposal recommendation and full branch address (at Part 3). Bundles of files should be clearly labelled and strapped or tied together.

If a receipt is required, e.g. for classified files, a MOD Form 24 (Receipt) containing the full branch address and contact telephone number must accompany each individual sack. If the branch is moving to a new address or being renamed, then the revised details should be included with the receipt.

Remember that only TOP SECRET material and material requiring special handling is to be sent to the Info-CMemR Sensitive Archive. All other material should be sent to the archive at Swandlincote.

### 3. Miscellaneous Material/Files/Records

Material not in registered files must be accompanied by a duplicate list of contents containing the branch name, address and telephone number. One copy will be retained at by the archive and the other returned as a receipt.

### 4. The address of the Info-CMemR Sensitive Archives is:

Old War Office, Room 012
Whitehall
London, SW1A 2EU

# Chapter 7 - Annex B

## Guidance on using The MOD Archive At Swadlincote

### 1. General Information

The following procedures should be complied with when either depositing or withdrawing files from TNT Archive at Swadlincote. General guidance is shown below but for full details please refer to the TNT Archive Services - Guide to Services that can be found on the Defence Intranet.

### 2. Records & Receipts

For all: registered files; material that is not in a registered file; or bundles of material the following procedures apply:

a. TNT Archive Services new business forms must be used. A copy should be sent with the records which will be returned by TNT to acknowledge receipt.

b. A record must be maintained of everything sent to the archives, including the date of despatch. TNT cannot provide a retrospective list of material sent. An additional copy of the TNT Archive Services new business form (see 2a above) would meet this requirement.

c. A MOD Form 24 for each SECRET Document, File, Bundle, or Sack (as appropriate) must be sent with full branch address and contact telephone number written/stamped on back. If the Branch is moving or being re-named, put the revised details on the receipt.

d. TOP SECRET material or material requiring special handling MUST NOT be sent to TNT Archive Services – It must be sent to the Info-CMemR Sensitive Archive in accordance with Chapter 7 Annex A.

e. MOD Form 24s must ONLY be sent for items classified as SECRET.

### 3. Registered Files

The following instructions for registered files apply in addition to those shown at paragraph 2 above:

a. The documents must be in Registered File covers – not Temporary Enclosure Jackets, branch folders, or bundles of loose papers, etc.

b. Each file must contain a completed MOD Form 262F showing: full file title and reference (e.g. prefix, file number and file part – where applicable) fully completed record of file review and destruction date (Part 2 of the form), a branch stamp including full address/telephone no: signature of reviewing officer of the correct grade (Band C2/Service equivalent or above).

c. A copy of the MOD Form 262F should be retained for the Branch record of all files archived at the TNT Archive.

d. Large large/bulky files are to be strapped; otherwise they may split/fall apart when opened and papers will be lost.

e. File titles/Numbers on covers are to be clearly legible.

f. Empty file covers containing no other papers should not be sent to the TNT Archive.

g. Records which are due to be destroyed imminently should not be sent to the TNT Archive.

**Files lacking details at paragraphs 3a and 3b above will NOT be accepted by TNT and will be returned to sender.**

### 4. Material not in Registered Files

This material should be sent with 2 copies of a list of contents using the new business forms. TNT Archive Services will keep one copy and return the other as a receipt.

This type of material must NOT be mixed with registered files. It is stored in a different section of the archive.

### 5. Bundles

Bundles of files or other material must be:

a. Clearly labelled; and

b. Strapped together with 2 copies of a list of contents.

# Chapter 8

## Public Access to Records less than 30 Years Old

### 8.1 Criteria for Access

The Freedom of Information Act 2000 (FOIA) provides legislative basis for public access to records which are not yet 30 years old, whether held by MOD or held, on a closed basis, by The National Archives; however, it is possible to exempt information from release by application of relevant exemptions under FOI. Guidance on the application of FOIA as issued by DG Information Access, can be found on the Defence Intranet: Respond to Requests for Information and Use the FOI Guidance.

### 8.2 Sponsored Access

"Privileged access", meaning the granting of special access to selected individuals, is inconsistent with the spirit of open government. Access by individuals should therefore only normally be approved if the individual is involved in research which is commissioned, sponsored or approved by MOD or is seen to be research from which HMG or MOD will derive benefit, and can be justified as being in the public interest. Such "sponsored access' can be agreed at the discretion of the business unit holding the records concerned.

Such access should only be approved if the work involved in making the appropriate records available does not detract significantly from the ongoing work of the business unit. In cases of doubt about the merit of allowing sponsored access, or for more detailed advice on the subject, please contact Info-CMemR.

RESTRICTED
DECLASSIFIED

Army Code 71038

# LAND COMPONENT HANDBOOK

# (SOHB)

Issue 1.0: July 2002

This Handbook replaces Army Code 71038 Staff Officers' Handbook of July 2000

DECLASSIFIED
RESTRICTED

DECLASSIFIED

## SERIAL 74A – OPERATIONAL RECORD (OR)

### Purpose

1. The OR is intended to capture as much information as practicably possible about the operations that a unit/formation conducts. If properly completed it should be possible to reconstruct events from the information contained in the OR. Once captured this information is used for a wide variety of purposes ranging from future training to settlement of pension claims.

### Introduction

2. Army Form C2119 – the Operational Record – lists what information is required and contains instructions on the format and maintenance of the OR for the duration of an operation. Much of the required information will be generated by the production of routine reports and returns. Where this is the case it is simply a matter of ensuring that two copies of these R2 are distributed to the relevant annex within the OR. (Note all references and distribution on existing forms to the Commander's Diary (Comd's Diary) should be changed to read OR).

3. The required information is stored within the OR by way of individual annexes listed on the C2119. Some information will be common to all ops, some will be specific to a particular type of operation. The format is designed to be generic but common sense and flexibility should be applied to ensure that as much significant information as possible is captured. Units and formations are encouraged to add additional annexes to those on the C2119 to suit the circumstances of each operation. For example, in OOTW/Peace Support Ops, separate annexes may be needed for Media/Information Operations and liaison with humanitarian organisations.

4. The OR process is overseen by Information – Analysis Branch at MOD Centre. Any advice or questions should be directed to them.

### General

5. ORs are required to be maintained by all formations, unit commanders and sub-unit/detachment commanders when so ordered.

6. At the formation level the OR is the responsibility of the COS, at unit level it is the responsibility of the second in command.

7. The OR is a 'living' document that is maintained for the duration of a deployment and is submitted back to MOD centre on a monthly basis. It should not be confused with post-operational reporting or Lessons Learned. If completed according to these instructions then the OR should function as a comprehensive resource for all post-op reporting and any post-op interviewing that takes place.

8. The C2119 therefore acts as a 'wrapper' within which all significant operational information (and *potentially* significant information) is stored. It is glued together by the completion of Annex A, the Chronological Overview (Army Form C2118). The CO should contain a chronological listing of all significant incidents detailing location, time and date.

DECLASSIFIED

DECLASSIFIED

and appropriate reference where the detailed information is held in the annexes. It is important that there is at least one daily entry, even if this is 'nothing significant to report' to ensure that there is a continuous chronological commentary.

9. Electronic copies of forms C2118 and C2119 are contained on the DGD&D 'Electronic Battle Box'. All of the detailed instruction for maintaining the OR is contained on the AFC 2119. Queries relating to the above procedure can be directed to Information-Analysis at 3-5 Great Scotland Yard, London SW1A 2HW, Tel:
r

DECLASSIFIED

**Authority**
Army Historical Branch

DECLASSIFIED

RESTRICTED

1

CLASSIFICATION

Army Form C2119

Original or Duplicate

2

# OPERATIONAL RECORD

| | | | | | |
|---|---|---|---|---|---|
| Unit/Formation | 3 | Operation | | From | 4 |
| | | Location | | To | |

## ANNEX LIST

| ANNEX | | | ENCLOSURE NUMBERS | | |
|---|---|---|---|---|---|
| A | Chronological Overview | 5 | | to | |
| B | Periodical Summary of Operations | | | to | |
| C | Watch Keepers Log (Original Required) | 6 | | to | |
| D | Messages Connected with Log | | | to | |
| E | Op Orders, FRAGOs, Warning Orders, Confirmatory Notes Issued | | | to | |
| F | Op Orders, FRAGOs, Warning Orders, Confirmatory Notes Received | | | to | |
| G | Sitreps and Combatreps Issued | | | to | |
| H | Orbats + Location Reps Issued | 7 | | to | |
| I | Intelligence Reports/Summaries Issued – Including IPB material | | | to | |
| J | Administrative Orders + Instructions Issued/Received | | | to | |
| K | All reports and returns required by unit and formation SOPs | | | to | |
| L | Ammunition + Field Strength Returns | | | to | |
| M | Nominal Rolls | 8 | | to | |
| N | Standing Orders | | | to | |
| O | Commanders Policy + Demi-Official Letters | | | to | |
| P | Action/Incident reports (To include Casualties (Personnel + Vehicle), POW + enemy Cas Ammunition expenditure) | | | to | |
| Q | Maps (including Battlemaps, overlays and Master Intelligence map) Diagrams, Air Photos | 9 | | to | |
| R | Detached/Sub-unit Sitreps | | | to | |
| S | Computer Files/E-mails (software used to be marked on box) | 10 | | to | |
| T | Meeting Reports + Written estimates | | | to | |
| V | Welfare/Deaths Injuries | | | to | |
| W | Major factors affecting significant decisions. Commander's opinions re equipment, tactics, morale, organisation etc | 11 | | to | |
| X | NBC/Environmental Incidents (including defensive measures) | 12 | | to | |
| Y | | | | to | |
| | | | | to | |
| Z | TOP SECRET SUPPLEMENTARY DIARY | 13 | | to | |

ED TO:-

ON

14

**Commander's Signature**

## COVERING LETTER 15

To: Ministry of Defence – DG Information (Exploitation) Analysis Branch/Historical Branch Army, Great Scotland Yard, London SW1 2HW

Reference No

1. I enclose Operational Record as detailed above

Appointment

2. Please return receipt below to acknowledge delivery

Signature

3. Please acknowledge receipt to this address:

CLASSIFICATION

DECLASSIFIED

RESTRICTED

**Authority**
Army Historical Branch

**Notes**

1. The classification of the OR should be determined by its contents rather than classification being predetermined and problematic information excluded. In most cases ORs are classified 'Secret'. Information must not be excluded from the OR on grounds of security as this will make reconstruction of events difficult if not impossible. The OR process is designed to cater for material classified 'Top Secret'. In circumstances where this threshold is insufficient contact Info-Analysis for advice.

2. Two copies of the OR are required. One (the original) must be submitted on a **monthly** basis to Information-Analysis. The second (duplicate) copy is retained by the unit/formation. This ensures that the unit/formation still has the information from the OR available and at the end of the deployment has a complete copy of the OR to use as a resource for post-op reporting.

3. Under normal circumstances records for sub-units will be maintained by the parent HQ. Where this is not practicable or the HQ is not present then sub-units must maintain an OR in line with these instructions. In any cases of doubt contact Info-Analysis.

4. ORs must be opened and maintained when a unit/formation is warned for operations. It is closed when a unit completes its operational deployment. (*Note: The OR is not a 'War Diary' that is opened and closed when hostilities start and finish.)* This ensures that issues, such as pre-op training, are properly documented.

5. It should be possible to use the CO to access all significant incidents/information in the OR annexes.

6. The original log (whatever its physical state) must form part of the monthly OR returned to Info-Analysis.

7. A comprehensive ORBAT should be included on the first month's OR. It can then be repeated or updated in subsequent months.

8. A comprehensive Nominal Roll must be included on the first month's OR. It can then be repeated or updated in subsequent months.

9. To allow reconstruction of events and location grids, copies of maps used must be included.

10. Use of IT in document preparation, e-mails and briefings is increasingly common within formation and unit HQs. Significant operational information on electronic format, not captured elsewhere, should be included in the OR normally by way of CD ROM. Where IT facilities allow, there is no reason why the entire OR should not be maintained and transmitted in a digital format. Where this is the case the software used to store the information must be detailed on the cover, the file structure should mirror the 2119 annex list and the individual files should have logical descriptors and date markings. The only part of the OR that must be sent 'hard copy' is the 2119 form itself, as this contains the CO's signature.

11. This is the section that allows a commander to explain rationale behind his decisions and comment on aspects of equipment, tactics, morale and organisation that impact on the operational deployment. In the case of long-term deployments this will mean that issues (good and bad) can be brought to attention quickly, rather than waiting for the conclusion of the operation. Detailed completion of this annex will inform a wide variety of users including the Lessons Learned and Post-Op interview teams.

12. An issue that arose from the 1991 Gulf War was the poor level of record keeping in respect of NBC incidents, potential exposures and defensive measures. As much detail as possible should be captured in respect of these matters. This section should also include any wider environmental information that may be potentially significant (eg proximity to burning oil wells).

13. Documents within the OR that are classified TOP SECRET are to be listed on the main C2119 OR cover, but grouped under cover of a supplementary C2119, protectively marked TOP SECRET. This is to be completed and clearly marked in red 'Annex Z'. This acts as the cover for the supplementary OR which is maintained in an identical way to the main OR but follows all the handling requirements for Top Secret material.

14. For legal reasons it is important that the CO sign the 2119. At present this original must be returned 'hard copy' to Info-Analysis.

15. This section provides Info-Analysis with the information required to send the originator a letter confirming receipt of the OR.

DECLASSIFIED

DECLASSIFIED

Army Form C2118
(Revised 2002)

This form will be enclosed with the annexes in AF C2119. If this is not available, the cover will be prepared in manuscript.

# Operational Record – Chronological Overview

Month and Year ____ Unit/Formation ____ Commanding Officer ____

| Place & Grid Ref | Day | Hour | Event or Information | Annex and Encl |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Authority**
Army Historical Branch

DECLASSIFIED

Army Code 71038

# LAND COMPONENT HANDBOOK

# (SOHB)

## AMENDMENT NO 1

## INSTRUCTION SHEET

1. **Delete**:

Page xv/xvi.

2. **Insert**:

a. New Page xv/xvi.

b. PART 3 – STAFF WORK
New Serial 74A Operational Record (OR) after Page 3-74-1.

3. Once the Amendment has been inserted, place this Instruction Sheet at the back of the publication.

DECLASSIFIED

RESTRICTED

# PART 3 – STAFF WORK

## SECTION 1 EQUIPMENT CAPABILITIES

## SECTION 2 STAFF PLANNING

DECLASSIFIED

DECLASSIFIED

## SECTION 3 OP STAFF DUTIES

DECLASSIFIED

DECLASSIFIED

## SERIAL 74A – OPERATIONAL RECORD (OR)

### Purpose

1. The OR is intended to capture as much information as practicably possible about the operations that a unit/formation conducts. If properly completed it should be possible to reconstruct events from the information contained in the OR. Once captured this information is used for a wide variety of purposes ranging from future training to settlement of pension claims.

### Introduction

2. Army Form C2119 – the Operational Record – lists what information is required and contains instructions on the format and maintenance of the OR for the duration of an operation. Much of the required information will be generated by the production of routine reports and returns. Where this is the case it is simply a matter of ensuring that two copies of these R2 are distributed to the relevant annex within the OR. (Note all references and distribution on existing forms to the Commander's Diary (Comd's Diary) should be changed to read OR).

3. The required information is stored within the OR by way of individual annexes listed on the C2119. Some information will be common to all ops, some will be specific to a particular type of operation. The format is designed to be generic but common sense and flexibility should be applied to ensure that as much significant information as possible is captured. Units and formations are encouraged to add additional annexes to those on the C2119 to suit the circumstances of each operation. For example, in OOTW/Peace Support Ops, separate annexes may be needed for Media/Information Operations and liaison with humanitarian organisations.

4. The OR process is overseen by Information – Analysis Branch at MOD Centre. Any advice or questions should be directed to them.

### General

5. ORs are required to be maintained by all formations, unit commanders and sub-unit/detachment commanders when so ordered.

6. At the formation level the OR is the responsibility of the COS, at unit level it is the responsibility of the second in command.

7. The OR is a 'living' document that is maintained for the duration of a deployment and is submitted back to MOD centre on a monthly basis. It should not be confused with post-operational reporting or Lessons Learned. If completed according to these instructions then the OR should function as a comprehensive resource for all post-op reporting and any post-op interviewing that takes place.

8. The C2119 therefore acts as a 'wrapper' within which all significant operational information (and *potentially* significant information) is stored. It is glued together by the completion of Annex A, the Chronological Overview (Army Form C2118). The CO should contain a chronological listing of all significant incidents detailing location, time and date,

DECLASSIFIED

DECLASSIFIED

and appropriate reference where the detailed information is held in the annexes. It is important that there is at least one daily entry, even if this is 'nothing significant to report' to ensure that there is a continuous chronological commentary.

9. Electronic copies of forms C2118 and C2119 are contained on the DGD&D 'Electronic Battle Box'. All of the detailed instruction for maintaining the OR is contained on the AFC 2119. Queries relating to the above procedure can be directed to Information-Analysis at 3-5 Great Scotland Yard, London SW1A 2HW, Tel:

DECLASSIFIED

**Authority**
Army Historical Branch

DECLASSIFIED

RESTRICTED

1

CLASSIFICATION

Army Form C2119

Original or Duplicate

2

# OPERATIONAL RECORD

Unit/Formation 3

Operation

Location

From 4

To

## ANNEX LIST

| ANNEX | | | ENCLOSURE NUMBERS | | |
|---|---|---|---|---|---|
| A | Chronological Overview | 5 | | to | |
| B | Periodical Summary of Operations | | | to | |
| C | Watch Keepers Log (Original Required) | 6 | | to | |
| D | Messages Connected with Log | | | to | |
| E | Op Orders, FRAGOs, Warning Orders, Confirmatory Notes Issued | | | to | |
| F | Op Orders, FRAGOs, Warning Orders, Confirmatory Notes Received | | | to | |
| G | Sitreps and Combatreps Issued | | | to | |
| H | Orbats + Location Reps Issued | 7 | | to | |
| I | Intelligence Reports/Summaries Issued – Including IPB material | | | to | |
| J | Administrative Orders + instructions Issued/Received | | | to | |
| K | All reports and returns required by unit and formation SOPs | | | to | |
| L | Ammunition + Field Strength Returns | | | to | |
| M | Nominal Rolls | 8 | | to | |
| N | Standing Orders | | | to | |
| O | Commanders Policy + Demi-Official Letters | | | to | |
| P | Action/Incident reports (To include Casualties (Personnel + Vehicle), POW + enemy Cas Ammunition expenditure) | | | to | |
| Q | Maps (including Battlemaps, overlays and Master Intelligence map) Diagrams. Air Photos | 9 | | to | |
| R | Detached/Sub-unit Sitreps | | | to | |
| S | Computer Files/E-mails (software used to be marked on box) | 10 | | to | |
| T | Meeting Reports + Written estimates | | | to | |
| V | Welfare/Deaths Injuries | | | to | |
| W | Major factors affecting significant decisions Commander's opinions re equipment, tactics, morale, organisation etc | 11 | | to | |
| X | NBC/Environmental Incidents (including defensive measures) | 12 | | to | |
| Y | | | | to | |
| | | | | to | |
| Z | TOP SECRET SUPPLEMENTARY DIARY | 13 | | to | |

14

Commander's Signature

ED TO:- ON

## COVERING LETTER 15

To: Ministry of Defence – DG Information (Exploitation) Analysis Branch/Historical Branch Army, Great Scotland Yard, London SW1 2HW

Reference No

1 I enclose Operational Record as detailed above

Appointment

2. Please return receipt below to acknowledge delivery

Signature

3. Please acknowledge receipt to this address:

CLASSIFICATION

DECLASSIFIED

744 - 8

RESTRICTED

Issue 1.1: Jan 03

**Authority**
Army Historical Branch

DECLASSIFIED
~~RESTRICTED~~

**Notes**.

1. The classification of the OR should be determined by its contents rather than classification being pre-determined and problematic information excluded. In most cases ORs are classified 'Secret'. Information must not be excluded from the OR on grounds of security as this will make reconstruction of events difficult if not impossible. The OR process is designed to cater for material classified 'Top Secret'. In circumstances where this threshold is insufficient contact Info-Analysis for advice.

2. Two copies of the OR are required. One (the original) must be submitted on a **monthly** basis to Information-Analysis The second (duplicate) copy is retained by the unit/formation. This ensures that the unit/formation still has the information from the OR available and at the end of the deployment has a complete copy of the OR to use as a resource for post-op reporting.

3. Under normal circumstances records for sub-units will be maintained by the parent HQ. Where this is not practicable or the HQ is not present then sub-units must maintain an OR in line with these instructions. In any cases of doubt contact Info-Analysis.

4. ORs must be opened and maintained when a unit/formation is warned for operations. It is closed when a unit completes its operational deployment. (*Note: The OR is not a 'War Diary' that is opened and closed when hostilities start and finish.)* This ensures that issues, such as pre-op training, are properly documented.

5. It should be possible to use the CO to access all significant incidents/information in the OR annexes.

6. The original log (whatever its physical state) must form part of the monthly OR returned to Info-Analysis.

7. A comprehensive ORBAT should be included on the first month's OR. It can then be repeated or updated in subsequent months

8. A comprehensive Nominal Roll must be included on the first month's OR. It can then be repeated or updated in subsequent months.

9. To allow reconstruction of events and location grids, copies of maps used must be included.

10. Use of IT in document preparation, e-mails and briefings is increasingly common within formation and unit HQs. Significant operational information on electronic format, not captured elsewhere, should be included in the OR normally by way of CD ROM. Where IT facilities allow, there is no reason why the entire OR should not be maintained and transmitted in a digital format. Where this is the case the software used to store the information must be detailed on the cover, the file structure should mirror the 2119 annex list and the individual files should have logical descriptors and date markings. The only part of the OR that must be sent 'hard copy' is the 2119 form itself, as this contains the CO's signature.

11. This is the section that allows a commander to explain rationale behind his decisions and comment on aspects of equipment, tactics, morale and organisation that impact on the operational deployment. In the case of long-term deployments this will mean that issues (good and bad) can be brought to attention quickly, rather than waiting for the conclusion of the operation. Detailed completion of this annex will inform a wide variety of users including the Lessons Learned and Post-Op interview teams.

12. An issue that arose from the 1991 Gulf War was the poor level of record keeping in respect of NBC incidents, potential exposures and defensive measures. As much detail as possible should be captured in respect of these matters. This section should also include any wider environmental information that may be potentially significant (eg proximity to burning oil wells).

13. Documents within the OR that are classified TOP SECRET are to be listed on the main C2119 OR cover, but grouped under cover of a supplementary C2119, protectively marked TOP SECRET. This is to be completed and clearly marked in red 'Annex Z'. This acts as the cover for the supplementary OR which is maintained in an identical way to the main OR but follows all the handling requirements for Top Secret material.

14. For legal reasons it is important that the CO sign the 2119. At present this original must be returned 'hard copy' to Info-Analysis.

15. This section provides Info-Analysis with the information required to send the originator a letter confirming receipt of the OR.

DECLASSIFIED
RESTRICTED

DECLASSIFIED
RESTRICTED

Army Form C2118
(Revised 2002)

This form will be enclosed with the annexes in AF C2119. If this is not available, the cover will be prepared in manuscript.

# Operational Record – Chronological Overview

Month and Year ______ Unit/Formation ______ Commanding Officer ______

| Place & Grid Ref | Day | Hour | Event or Information | Annex and Encl |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

DECLASSIFIED

RESTRICTED

**Authority**
Army Historical Branch

DECLASSIFIED
RESTRICTED

Not to be communicated to anyone outside HM Service without authority

LANDSO
1120

# LAND COMMAND

## STANDING ORDER NO 1120

by

GENERAL SIR RICHARD DANNATT

KCB CBE MC

Commander in Chief Land Command

## OPERATIONAL RECORD KEEPING (ORK)

WILTON
OCTOBER 2005

POC SO3 G3 Ops/Cts
(

DECLASSIFIED
RESTRICTED

# LAND COMMAND STANDING ORDER NO 1120

## OPERATIONAL RECORD KEEPING (ORK)

References:

A. QR Army 5.555 Operational Record.
B. AFSOP 410 Operational Record.
C. Land Component Handbook Part 1 Serial 74A (2003).
D. Army Field Manual Volume 1 Part 8 Command and Staff Procedures.
E. JSP 441 – Record Keeping.
F. JWP 3-00 Joint Operations Execution (2nd Edition).
G. AF C2118/C2119.
H. D/DGD&D/1/128 dated 20 Feb 02.

### INTRODUCTION

1. It is a legal requirement that units and formations maintain a record of their activities whilst deployed on operations (including Operations in the UK). This record provides evidence of actions and decisions which may later be the object of disciplinary investigation. The record also provides protection to units and commanders against litigation. It also assists with a wide range of Ministry of Defence activity from the validation of war pension claims, to the compilation of official histories. This process is known as Operational Record Keeping (ORK).

2. ORK is mentioned in a number of separate documents (References A-F). This LANDSO draws on all references and articulates current HQ LAND direction to Formations and Units as to the ORK process which they must follow.

### PURPOSE

3. The Operational Record (OR) is intended to capture as much relevant information as possible about the operations that a unit or formation conducts and is a chronological record of a units or formations preparation and deployment. It should be possible to reconstruct events from the information contained in the OR. Absence or inconsistent capture of information can have a negative impact on individuals, the Army and the MOD.

4. The intention of the OR is to provide the structured archiving and storage of all important documents and information produced as part of the normal routine staff process during operations.

### BATTLE RHYTHM

5. **Enduring Operations**. The OR should be opened and maintained on receipt of the Force Generation Signal issued by HQ LAND approximately 6 months prior to deployment. It should be closed when a unit or formation completes its operational deployment (the OR is not a 'war diary' which is opened and closed when hostilities start and finish). This ensures that the preparations for deployment are properly documented and may be referred to at a later date.

DECLASSIFIED
RESTRICTED

6. **JRRF/VHRR Forces**. Units/Formations held at readiness to deploy on operations should open and begin maintaining their OR when warned for a specific operation. It is closed when a unit or formation completes its operational deployment. Any issues outside the warning period during training should be captured using the routine unit or formation Historical Record.

7. **UK Operations**. An OR is to be maintained by units or formations deployed on Operations in the UK. This differs from overseas deployments in that units or formations may be warned for a deliberate operation, involved in routine operations or deployed with no notice in reaction to events in the UK. The following procedures apply:

a. **Deliberate UK Operations**. For a deliberate UK operation, units or formations should open and begin maintaining an OR when warned for the operation. The OR is to be closed when the operation has been completed and all force elements recovered.

b. **Routine UK Operations**. For routine UK operations such as Op MIDWAY, an OR is to be routinely maintained by the units involved. This is to be a constant process whilst units hold elements at readiness. The OR should include detail on operation specific training and licensing.

c. **Short Notice UK Operations**. For short notice UK operations (eg an emergency under Military Aid to the Civil Community (MACC) Category A arrangements) an OR should be opened and maintained from the moment the request for military support is made. It is to be closed when the operation has been completed and all force elements recovered.

8. **Submission**. ORs must be submitted (in either hard or soft copy) at the end of each calendar month to DG Information Corporate Memory (Army). DG Information Corporate Memory (Army) is the custodian of the OR process and retain ORs once completed. Completed ORs should be sent to:

Corporate Memory (Analysis)
DG Information
Floor 6 Zone G
Ministry of Defence Head Office
C O TNT
Pages Walk
Bermondsey
London SE1 4SB

Tel:
Fax:

9. **Monitoring Process**. Corporate Memory maintains a monthly record of returns from units. At the beginning of the third week of every calendar month, a list of units which have failed to send in their OR for the previous calendar month, or whose OR is inadequate, will be sent to Cts Div at HQ LAND. Cts Div will then ensure that the unit(s) concerned provides an OR for the missing period or updates the OR to the required standard. If a Unit fails to provide any OR for a 2 month period ACOS Cts will write to the Commanding Officer of that unit (copied to the chain of command) requiring a written explanation.

DECLASSIFIED
RESTRICTED

## RESPONSIBILITIES

10. ORs are required to be maintained by all formations, units and sub-units/detachments if deployed independently. It is the responsibility of the Formation Commander for Formations, the Commanding Officer for Units and Officer Commanding for Sub-Units[1] to ensure that the OR is maintained and sent to Corporate Memory at the end of each calendar month. The Commander is to sign the Army Form C2119.

## FORMS TO BE USED

11. **Army Form C2119**. Army Form C2119 (attached at Enclosure 1) lists the information required in the OR. Instructions on the format and maintenance of C2119 are below. The C2119 acts as a 'wrapper' within which all operational information (and potentially significant information) is stored. The OR format is designed to be generic but common sense and flexibility should be applied to ensure that as much significant information as possible is captured. Units and formations are encouraged to add additional annexes to those on the C2119 to suit the circumstances of each operation.

12. **Notes for Completion of Army Form C2119**. Notes to aid in completing the form are:

a. **Classification**.

(1) The classification of the OR should be determined by its contents rather than classification being pre-determined and problematic information excluded. In most cases ORs are classified SECRET. Information must not be excluded from the OR on grounds of security as this will make reconstruction of events difficult if not impossible.

(2) **TOP SECRET**. Documents within the OR that are classified TOP SECRET are to be listed on the main C2119 OR cover, but grouped under cover of a supplementary C2119, protectively marked TOP SECRET. This is to be completed and clearly marked in red 'Annex Z'. This acts as the cover for the supplementary OR which is maintained in an identical way to the main OR but follows all the handling requirements for TOP SECRET material.

b. **Number of Copies**. Two copies of the OR are required. One (the original) must be submitted on a monthly basis to Corporate Memory. The second (duplicate) copy is retained by the unit/formation. This ensures that the unit/formation still has the information from the OR available and at the end of the deployment has a complete copy of the OR to use as a resource for post-op reporting.

c. **Chronological Overview**. It should be possible to use the Chronological Overview to access all significant incidents/information in the OR annexes.

[1] In cases where a sub-unit is deployed independently and is required to maintain its own OR.

d. **Watchkeeper and Radio Logs**. The original watchkeeper and radio logs (whatever their physical state) must form part of the monthly OR returned to DG Information Corporate Memory/Historical Branch Army.

e. **ORBAT**. A comprehensive ORBAT should be included on the first OR, it can then be repeated or updated in subsequent months.

f. **Nominal Roll**. A comprehensive Nominal Roll must be included on the first OR, it can then be repeated or updated in subsequent months.

g. **Maps**. To allow reconstruction of events and location grids, copies of maps used must be included.

h. **IT**. Use of IT in document preparation, e mails and briefings is increasingly common within formation and unit HQs. Significant operational information on electronic format, not captured elsewhere, should be included in the OR normally by way of CD ROM. Where IT facilities allow, there is no reason why the entire OR should not be maintained and transmitted in a digital format. Where this is the case the software used to store the information must be detailed on the cover; the file structure should mirror the C2119 annex list and the individual files should have logical descriptors and date markings. The only part of the OR that must be sent 'hard copy' is the C2119 form itself (with the Commanders signature for legal reasons) and the logs.

i. **Annex W - Major Factors Affecting Significant Decisions**. This is the section that allows a commander to explain the rationale behind his decisions and to comment on aspects of equipment, tactics, morale and organisation that impact on the operational deployment.

j. **Annex X - NBC/Environmental Issues**. An issue that arose from the 1991 Gulf War was the poor level of record keeping in respect of NBC incidents, potential exposures and defensive measures. As much detail as possible should be captured in respect of these matters. This section should also include any wider environmental information that may be potentially significant (eg proximity to burning oil wells).

13. **Army Form C2118**. The OR is 'glued' together by the completion of Army Form C2118, the Chronological Overview (attached at Enclosure 2). The Chronological Overview should contain a chronological listing of all significant incidents detailing location, time and date, and appropriate reference where the detailed information is held in the Annexes. It is important that there is at least one daily entry, even if this is 'nothing significant to report', to ensure that there is a continuous chronological commentary. Instructions on the format and maintenance of C2118 are below.

14. **Notes for Completion of Army Form C2118**.

a. The chronological overview is to record the following information directly or in the appropriate annex:

(1) Changes in Command, Location (by location and map reference), Establishment, Equipment, Organisation.

(2) Short summary of each day's fighting/operations, including sub-unit movement and location.

(3) Information received, decisions made, orders given.

(4) Weather, ground conditions and general environment when relevant.

(5) Progress of defensive works.

(6) Weapon state.

(7) Casualties to personnel and vehicles with major causes.

(8) Enemy prisoners and equipment captured.

(9) Statement showing how the unit was employed in the time not otherwise accounted for. If this is training then the training type should be specified.

(10) Opinions and recommendations of the commander with regard to equipment, tactics, organisation and morale.

(11) Major factors affecting significant decisions.

b. To be of genuine value the contents have to be accurate, honest and objective. Authors should avoid the temptation to exclude unpalatable facts, particularly in respect of Annex W.12.

15. **Electronic Copies**. Electronic copies of forms C2118 and C2119 are contained on the DGD&D 'Electronic Battlebox', which can be found on the MOD Intranet at http://bacbb.asei.mod.uk/.

16. **Related Documents**.

a. **Unit/Formation Historical Records**. The production of the OR should not change this process. During times when the OR is being maintained, the second copy retained by the unit, becomes the Historical Record.

b. **Post Operational Tour Report (POR)**. The OR should not be confused with the POR, which must be submitted on conclusion of the operation using the DGD&D Generic Army POR/PXR Format at Reference H. The POR may draw upon information held in the OR, but the POR is intended to inform the LAND Lessons Action Plan (LLAP).

c. **Post Training Report (PTR)**. Similarly, the OR should not be confused with the PTR, which must be submitted no later than 2 months after deploying. The PTR may draw upon information held in the OR, but the PTR is intended to inform HQ LAND Trg Branch, LWC and OPTAG, in order that they can identify the key strengths and weaknesses of Pre-Deployment Training.

## SUMMARY

17. The purpose of the OR is to provide a factual summary of key events and decisions in the course of an operation. It needs to be sufficiently comprehensive to enable events to be accurately reconstructed and understood, even some time afterwards. Besides being a matter of professional pride, the rigorous keeping of an OR will provide valuable protection for commanders and soldiers against false or malicious allegations.

B W B WHITE-SPUNNER
Maj Gen
for CinC

Enclosures:

1. Army Form C2119.
2. Army Form C2118.

ENCLOSURE 1

CLASSIFICATION DECLASSIFIED

Army Form C2119

Original or Duplicate

## OPERATIONAL RECORD

| | | | | | |
|---|---|---|---|---|---|
| Unit<br>Formation | | Operation | | From | |
| | | Location | | To | |

### ANNEX LIST

| ANNEX | | ENCLOSURE NUMBERS | | |
|---|---|---|---|---|
| A | Chronological Overview | | to | |
| B | Periodical Summary of Operations | | to | |
| C | Watch Keepers Log (Original Required) and Radio Logs | | to | |
| D | Messages Connected with Log | | to | |
| E | Op Orders, FRAGOs, Warning Orders, Confirmatory Notes Issued | | to | |
| F | Op Orders, FRAGOs, Warning Orders, Confirmatory Notes Received | | to | |
| G | Sitreps, Combatreps and Patrol reports Issued | | to | |
| H | Orbats – Location Reps Issued | | to | |
| I | Intelligence Reports-Summaries Issued – Including IPB material | | to | |
| J | Administrative Orders + Instructions Issued Received | | to | |
| K | A 1 reports and returns required by higher unit and formations | | to | |
| L | Ammunition + Field Strength Returns | | to | |
| M | Nominal Roles | | to | |
| N | Standing Orders | | to | |
| O | Commanders Policy & Letters | | to | |
| P | Action/Incident reports (To include Casualties( Personnel + Vehicle), POW + enemy Cas Ammunition expenditure) | | to | |
| Q | Maps (including Battlemaps, overlays and Master Intelligence map) Diagrams, Air Photos | | to | |
| R | Sub-unit Sitreps | | to | |
| S | Computer Files E-mails (software used to be marked on box) | | to | |
| T | Meeting Reports + Written estimates | | to | |
| V | Welfare Deaths, Injuries | | to | |
| W | Major factors affecting significant decisions, Commander's opinions re. Equipment, Tactics, Morale, organisation etc | | | |
| X | NBC Environmental Incidents (including defensive measures & policy docs) | | to | |
| Y | | | to | |
| | | | to | |
| Z | TOP SECRET SUPPLEMENTARY DIARY | | to | |

DESPATCHED TO: ON

Commander's Signature

### COVERING LETTER

To: Ministry of Defence - DG Information Corporate Memory/Historical Branch Army, Floor 6 Zone G, MOD – Head Office, c/o TNT, Pages Walk, Bermondsey, London SE1 4SB

Reference No

1. I enclose Operational Record as detailed above

Appointment

2. Please return receipt below to acknowledge delivery

Signature

3. Please acknowledge receipt to this address

CLASSIFICATION DECLASSIFIED

DECLASSIFIED

ENCLOSURE 2

Army Form C2118
(Revised 2002)

This form will be enclosed with the annexes in AF C2119. If this is not available, the cover will be prepared in manuscript.

# Operational Record – Chronological Overview

Month and Year ______ Unit/Formation ______ Commanding Officer ______

| Place & Grid Ref | Day | Hour | Event or Information | Annex and Encl |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

DECLASSIFIED

DECLASSIFIED

Issued: April 2011

Superseding: BR 9461

Dated: 2008

# BRd 9461

## OPERATIONAL & HISTORICAL RECORD KEEPING POLICY FOR THE NAVAL SERVICE

THIS DOCUMENT IS THE PROPERTY OF HER BRITANNIC MAJESTY'S GOVERNMENT and is issued for the information of such persons only that need to know its contents in the course of their official duties. Any person finding this document should hand it to a British Forces unit or to a police station for its safe return to the Ministry of Defence. DDef Sy Main Building Whitehall LONDON SW1A 2HB, with particulars of how and where found.

THE UNAUTHORISED RETENTION OR DESTRUCTION OF THE DOCUMENT IS AN OFFENCE UNDER THE OFFICIAL SECRETS ACTS OF 1911-1989 (When released to persons outside government service, this document is issued on a personal basis and the recipient to whom it is entrusted in confidence, within the provisions of the Official Secrets Acts 1911 1989 is personally responsible for its safe custody and for seeing that its contents are disclosed only to authorized persons)

By Command of the Defence Council

DECLASSIFIED

DECLASSIFIED

COMMANDER-IN-CHIEF FLEET

## SPONSOR INFORMATION

This publication is sponsored by the Fleet Desk Officer identified below on behalf of **Commander in Chief Fleet**.

FLEET-OPS-WO OPS
Fleet Operations
Oswald Building
Building 470
Northwood HQ
Sandy Lane
Northwood
HA6 3HP
E-mail FLEET-OP POL MOD SO2
Tel

This publication is authored and published by the **Fleet Publications and Graphics Organisation (FPGO).**

The Officer responsible for this publication is:

OIC FPGO
Pepys Building
HMS COLLINGWOOD
Fareham
Hants
PO14 1AS
RLI e-mail: fsag-pfsa
Tel

All correspondence concerning this publication is to be forwarded to the FPGO Author/ Responsible Officer and copied to the Fleet Desk Officer.

© UK MOD Crown Copyright 2011

DECLASSIFIED

DECLASSIFIED

## RECORD OF CONFIGURATION CONTROL

| | Authored by | Checked by | Approved by |
|---|---|---|---|
| Edition/Change:<br>Date of edition/ change: | Name:<br>Tally:<br>FSA CS2<br>Signature:<br>Signed on File Copy<br>Date:<br>1 April 11 | Name:<br>Tally:<br>HA<br>Signature:<br>Signed on File Copy<br>Date:<br>1 April 11 | Name:<br>Tally:<br>FLEET-OP POL MOD SO2<br>Signature:<br>Signed on File Copy<br>Date:<br>1 April 11 |
| Edition/Change:<br>Date of edition/ change: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: |
| Edition/Change:<br>Date of edition/ change: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: |
| Edition/Change:<br>Date of edition/ change: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: |
| Edition/Change:<br>Date of edition/ change: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: |
| Edition/Change:<br>Date of edition/ change: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: |
| Edition/Change:<br>Date of edition/ change: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: | Name:<br>Tally:<br>Signature:<br>Date: |

DECLASSIFIED

DECLASSIFIED
UK RESTRICTED

## PROPOSALS FOR CHANGES

Protective Marking: ..........................................................................

Ship / Establishment: ........................ Originating Dept: ........................ Date: ...................

| | |
|---|---|
| Title of Publication: | BRd 9461 |
| Current Issue Status: | April 2011 |

DETAILS OF COMMENTS

| Para | Para Number | Comment: |
|---|---|---|
| | | Continue of separate sheet if required. |

| | |
|---|---|
| Originator:<br>(Name in Block Letters) | Head of Department:<br>(Name in Block Letters) |
| Signature: | Signature: |
| Rank / Rate: | Rank/Rate: |

Protective Marking:

UK RESTRICTED
DECLASSIFIED

DECLASSIFIED

## PREFACE

## COMMANDER OPERATIONS

The subject of Operational Records is not new. Royal Navy units have always been required to produce them, and for obvious reasons: learning from experience allows us to make decisions, and strengthens our ability to fight in the future. If we are able to demonstrate our record of achievement, we will make more convincing arguments for resources.

The requirement for Operational Records is currently reinforced by both legal obligations, and our duty to our personnel. Accurate records allow important issues, such as medal entitlement, and pension and compensation claims, to be resolved as quickly and fairly as possible. *Records have been and continue to be utilised in supporting the cases for Naval Service manning, operational capability and Worldwide tasking. Most recently, in 2010, records archived at the Naval Service Historical Branch were utilised in the SDSR process.*

For centuries the Royal Navy has been able to demonstrate an enviable and unequalled record of achievement. It is essential that this tradition continues.

Rear Admiral
COMOPS

DECLASSIFIED

DECLASSIFIED

## CONTENTS

DECLASSIFIED

DECLASSIFIED

# CHAPTER 1

## INTRODUCTION

## ANNEXES

DECLASSIFIED

## CHAPTER 1

## INTRODUCTION

### 0101. Why Operational and Historical Records?

a. The keeping of Operational Records is an ***enduring legal requirement*** for all Britain's Armed Forces. These records are an essential aspect of the future operational capability of the Naval Service. Missing or inadequate records create operational, legal, and financial risks. Comprehensive and accurate records inform improved decision making and the best investment choices.

b. Immediate **Operational Reports**, such as Post Deployment Reports, or RFA State of the Nation reports, provide direct feedback to FLEET HQ to improve operational performance. They also inform the wider joint and combined defence community on current themes and issues, allowing the argument for maritime effects to be properly represented in the Centre.

c. These vital records, *up to and including Top Secret Strap 3*, are managed by the Naval Historical Branch (NHB) within CNS Area. Operational Records arriving in NHB are analysed to provide evidence to policy makers across Defence. They ensure that maritime issues remain in the vanguard of defence policy, and enhance decisions on future procurement and training.

d. To provide a complete picture of naval activity, there is a defence requirement for more than just Operational Reports. **Unit Records**, the combination of Operational Reports with supporting documentation, such as Sitreps or ship's investigations, are maintained for every unit within the Naval Service. The records are required to enable studies and operational analysis, *provide evidence for Service Police investigations*, provide evidence for medal entitlements, or to deal with claims from the Veterans Agency. *For example, should an incident occur in a Naval Service unit, which even decades after the event, becomes a litigation case against the Ministry of Defence, Unit Records will be utilised as a reliable source of accurate historical information. The Naval Historical Branch also deals with enquiries from potential conspiracy theorists who, finding a gap in historical documentation, speculate that a unit was involved in some activity other than it actually was. The Unit Records provide evidence to counter potentially damaging speculation.*

e. In producing accurate records of their operational activity, each unit is maintaining its reputation and creating its own historical legacy. In contrast to virtually every other unit return, the Unit Records will be permanently preserved. They will remain as an enduring testimony to the achievement of the personnel of each unit in the Naval Service.

### 0102. General Policy Principles

a. **Introduction**. Commander (Operations) [COMOPS] has the legal responsibility to ensure accurate records are kept by all operational units and staffs of the Naval Service. In order to do this all Naval Service units, Battlestaffs and Naval Parties must adhere to the following reporting policy. *The general instructions detailed in this section apply to all units within the Naval Service. Specific, additional, requirements can be found within annexes to this document for each Naval Service area which provide a tailored reporting structure.*

DECLASSIFIED

b. **General Instructions**. These are to be Applied by all Naval Service Units and Battlestaffs as Listed on the Fleet Bridge Card. With the exception of Fleet Shore Units, Units without Naval Service personnel embarked and Units under other Service Full Command ie Army.

c. *Previous vehicles through which units recorded/reported their activities did not meet the need to provide an accurate narrative of unit activity, nor did they provide the appropriate level of feedback for the HQ on completion of operational deployments.* In order to meet the modern requirement, this process is now divided into 2 related but distinctly separate elements that all units have to satisfy as routine business.

d. **Unit Narrative**. As of 1 November 2007 the ROP *was* discontinued and replaced by the requirement for every unit to complete a Monthly Unit Record (MUR). Unit activity is to be summarised each month and using the baseline template document, the appropriate signature level *signed off by the* ***Commanding Officer*** *or* ***Chief of Staff****. This monthly requirement is enduring and must be conducted regardless of the activity the unit is engaged in provided Naval Service Personnel are embarked – this includes for example refit periods and POTL. For ships in dormancy, ie no personnel onboard, a collective record is to be submitted on behalf of the dormant ship(s) by host ships. If there is no host ship, the last MUR submitted by the unit to be dormant must indicate the scheduled period of dormancy.* The MUR satisfies the legal requirement for each unit to produce an accurate narrative of the unit's activities for formal archiving. The MUR Summary records a timeline of unit activity for each month as well as recording highlights and Command Comments, emphasising programme milestones and the unit's effectiveness against its directed tasks. This record compliments the Fleet Operational Capability [FLOC] return which supports OC assessments and future forecasting.

e. The one page MUR Summary is to be supported by a number of mandatory enclosures that must be collated by the unit during the calendar month *including, when required, documents which demonstrate/evidence that "actions were appropriate" (JSP 747 Protocol 010 para. 7. refers)* The MUR is designed to capture documentation produced from existing processes/routines *in order that the evidence of the activities that took place and associated decisions taken is not lost.* It will provide the necessary documentary information to support the work of the Naval Historical Branch (NHB) as the corporate memory for the Naval Service. The mandatory enclosures required are different for each FLEET area and full details can be found within the specific instructions detailed later in this document.

f. The MUR is to be completed monthly and despatched by the 15th of the following month. The despatch should be made in electronic *form* when possible *(via CSS, Email, DVD or CD-ROM following rules laid down in JSP 440 where appropriate)*, or in hard copy if not possible. Any inability to submit a MUR must be signalled to MODUK NAVY for CNS NHB HS3, the signal should include the circumstances and the unit's estimate of when the required MUR(s) will be submitted.

DECLASSIFIED

g. **Operational Records**. In addition to the enduring MUR requirement, units will still be required to submit operational reports as directed by their Operational Commander on completion of specific operational activities. These reports differ from the MUR in that they are targeted at providing direct feedback on the conduct of operational activity. They allow COs to make observations and comments that are invaluable in improving operational performance. This requirement also removes the need for the FLEET HQ to trawl through the MURs for operational feedback. All lessons that are identified are to be submitted to the Fleet Lessons Management System in accordance with the latest MWC OKX guidance. Identifying lessons in Operational Reports or MUR does not negate the requirement to submit lessons to FLMS. *The requirement for an Operational Report does not negate the requirement for units to maintain concurrent records through the MUR process.* Operational reports fall into 3 broad categories and current guidance concerning their content and submission from Operational Commanders remains extant.

(1) *Post Deployment Reports (PDRs).* These reports are to be submitted by all ships (including RFA), submarines (termed a Patrol Report) and detached Squadrons on completion of specific deployments (APT, TELIC, CALASH, NATO, CHOBDAHAR etc). The requirement for producing such documents will be confirmed in appropriate Mission Directives/Oporders.

(2) *Post Operation Reports (PORs)/Operational Records.* These reports are to be submitted by Royal Marine units on completion of operational deployments as part of a Land Component (HERRICK, TELIC etc).

(3) *Post Exercise Reports (PXRs).* These are to be submitted by all units taking part in specific exercise activities as detailed in appropriate exercise instructions.

h. Addressees for Operational Records will be detailed in operational orders/directives but the following addressees must be included as standard. *Copies of Operational Records are to be included as a Mandatory Enclosure to the MUR.*

PDRs/PORs.
The appropriate Operational Commander
FLEET - CINCFLEET
FLEET - COMOPS
FLEET - COS CAP
Director MWC for OKX.
PORFLOT/DEVFLOT/FASFLOT as appropriate
FOST

PXRs.
FLEET - CINCFLEET
FLEET - COMOPS
FLEET - COS CAP
Director MWC for OKX.
PORFLOT/DEVFLOT/FASFLOT as appropriate
FOST

i. **Classification**. It is vital that the Royal Navy should have a complete record of its activities. The Naval Historical Branch is therefore cleared and authorised to hold material classified up to and including Top Secret Strap. All material below Top Secret Strap 3 is to be included in the MUR. Any exclusions of material of a higher classification must be noted in the MUR cover sheet, with reference to where the material has been submitted, i.e. DI(Ops). Material of Secret and above will be security receipted as normal.

DECLASSIFIED
UK RESTRICTED

j. **Acknowledgement, Use and Monitoring**. MURs' will be acknowledged by *NHB within 10 working days.* However, to ensure maximum availability of their valuable content the MUR Summaries will, as far as possible, be available for viewing through the Unit Capability Reports (UCR) of FLEETWEB, in addition to their distribution to MWC and NHB. The enclosures can then be accessed via the UCR or the NHB as appropriate. NHB is also required to make periodic reports on MUR submissions to both COMOPS and ACNS. These observe trends and highlight both particularly valuable submissions and any gaps in submission, in order that future risks to RN resources can be identified and promptly addressed. *MURs will be assessed as part of the FOST IM audit process. Fleet Operations, Northwood is responsible for policing the timely submission of Unit Records and will actively pursue Units failing to comply with instructions contained herein.*

k. **Points of Contact**. The NHB retain responsibility for archiving the material submitted and questions should be addressed directly. The NHB POC is CNS NHB HS3 Email cnsnhbhs3@a.dii.mod.uk, CNS-NHB-HS3.). The FLEET POC for all units if required is Fleet Op Pol MOD SO2 at Northwood (Tel: Email: will change to ).

## ANNEX 1A

## SURFLOT & RFA SPECIFIC INSTRUCTIONS

1. **Application.**
This requirement applies to all surface units of the Royal Navy and the Royal Fleet Auxiliary including units under Commander 1 Patrol Boat Squadron.

2. **Narrative Requirement.**
Units are to complete a Monthly Unit Record (MUR) with associated Mandatory Enclosures as prescribed in the General Instructions with the following specific caveats.

a. Ships with embarked Flights are to include a copy of the Flight MUR with their own to provide a complete record. For months where the aircraft is disembarked, the Flight will submit its MUR through the parent Squadron's MUR.

b. Units with full Naval Air Squadrons or Naval Air Squadron detachments embarked are to include copies of the Squadron/Detachment's MUR with their own. If not embarked Squadrons will follow separate procedures detailed in this document.

c. ***MCMV Crew Rotation****. Crews embarked are responsible for MURs for that platform. When it is known that a platform is to go dormant during a crew RIP, the appropriate authorities should be notified in the last MUR submitted before dormancy.*

d. 1 PBS Units *(URNU)* are to submit their *Monthly Status Reports (MSR)* to Squadron Headquarters for collation by Squadron staff before despatch to the NHB. *NHB accepts the MSR in lieu of the MUR as it fulfils all current requirements. All other Patrol Boats are to submit an MUR in accordance with the general instructions.*

e. Ships with Royal Marine Protection/Boarding Teams or Boat Groups are to include a copy of the Team's MUR within their own monthly submission.

f. As part of the monthly submission, all units are to include the following Mandatory Enclosures with their MUR submission:

(1) Any Operational Reports submitted within the calendar month, including RFA 'State of the Nation' Reports (see General Policy Principles, Para 4).

(2) OSREPS/ASSESSREPS

(3) Weekly Sitreps provided to FLEET HQ whilst deployed.

(4) Ship's Investigations.

(5) Casualty & Incident Signals/Reports.

(6) POLREP Signals.

(6) A25 reports.

(7) Reports on Collisions and Groundings.

(8) Souls on Board Report (Aggregated monthly list of all personnel serving onboard for more than 24 hours).

DECLASSIFIED
UK RESTRICTED

(9) Operational Sea Training final assessment signal.

(10) Summary of Lessons raised to FLMS.

Additionally for all units:

(11) Any other signal or document deemed of interest or significance to the historical record of the ship.

g. **Submission & Distribution.** The MUR is to be despatched by the 15th of the following month to the distribution list below:

| Organisation | Electronic Address for Submissions | Physical Address for Submissions | Content |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP 20, NMHB Portsmouth, PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator, Mail Point 2-4, Sir Henry Leach Building, Whale Island, Portsmouth, PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

3. **Operational Records.**

On completion of any operational activity, units are to submit PDRs/PORs/PXRs as instructed in relevant directives/exercise instructions complying with the instructions detailed in the General Instructions section of this document.

**CLASSIFICATION (to be completed)**

MUR SUMMARY – SURFLOT & RFA

UNIT:

MONTH & YEAR:

SUMMARY OF UNIT ACTIVITY:

To include Command State, including any changes with date; operations, exercises and trails undertaken with dates and brief description; significant incidents, such as accidents or serious injuries, & major events such as VIP visits and industry days

**CLASSIFICATION (to be completed)**

DECLASSIFIED
UK RESTRICTED

CLASSIFICATION (to be completed)

| MANDATORY ENCLOSURES | Number |
|---|---|
| Operational reports (including State of the Nation reports) | |
| OSPREPS/ASSESSREPS | |
| Weekly Sitreps | |
| Ships Investigations | |
| Casualty & Incident signals/reports | |
| POLREP signals | |
| A25 reports | |
| Reports on Collisions and Groundings | |
| Souls on Board reports | |
| OST final assessment signals | |
| Summary of Lessons raised to FLMS | |
| Any other significant documents | |

COMMAND COMMENTS

Comments should include programme milestones & the unit's effectiveness against its directed tasks and during Port Visits. Command should also approve the MUR, explicitly confirming any security exclusions & identifying the custodians of these exclusions.

SUBMISSION & DISTRIBUTION

| ORGANISATION | ELECTRONIC ADDRESS FOR SUBMISSIONS | PHYSICAL ADDRESS FOR SUBMISSIONS | CONTENT |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP20, HMNB Portsmouth, PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator, Mail Point 2-4, Sir Henry Leach Building, Whale Island, Portsmouth, PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

CLASSIFICATION (to be completed)

## ANNEX 1B

## SUBFLOT SPECIFIC INSTRUCTIONS

1. **Application**.
This requirement applies to all submarines of the Royal Navy including SSBNs.

2. **Two Crews**.
In the case of submarines with more than one crew, MURs are to be submitted by the 'On' crew (currently embarked and with ownership of the platform). It is appreciated that, in most circumstances, submarines will be unable to communicate their MUR's whilst deployed; however the MUR backlog should be communicated to the appropriate authorities as soon as possible on return from patrol. MUR's should make it clear which crew is embarked at the time of the monthly submission

3. **Narrative Requirement.**
Submarines are to complete a Monthly Unit Record (MUR) with associated Mandatory Enclosures as prescribed in the General Instructions with the following specific caveats.

a. The requirement to submit a MUR does not remove or duplicate the reporting requirements for SUBFLOT as detailed in FPN 017. These continue to be required for distinct and immediate technical and analytical purposes, rather than as the permanent record of all aspects of unit activity.

b. As noted in Paragraph 6 of the General Policy Instructions, it is vital that the Royal Navy should have a complete record of its activities. The Naval Historical Branch is therefore cleared to hold material classified up to and including Top Secret Strap. **All material below Top Secret Strap 3 is to be included in Subflot MURs**. Any exclusions of material of a higher classification must be noted in the MUR cover sheet, with reference to where the material has been submitted, ie DI(Ops), SSPAG.

c. As part of the monthly submission, all units are to include the following Mandatory Enclosures with their MUR submission:

(1) Any Operational Reports submitted within the calendar month (see General Policy Principles, Para 4).

(2) OSREPS/ASSESSREPS

(3) Weekly Unit Sitreps provided to FLEET HQ whilst deployed.

(4) Ship's Investigations.

(5) Casualty & Incident Signals/Reports.

(6) POLREP Signals.

(7) Reports on Collisions and Groundings.

(8) Souls on Board reports.

(9) Operational Sea Training final assessment signal.

(10) Summary of Lessons raised to FLMS [See RNTM 141/07].

DECLASSIFIED ~~UK RESTRICTED~~

Additionally for all submarines:-

(11) Any other signal or document deemed of interest or significance to the historical record of the submarine.

d. **Submission & Distribution**. The MUR is to be despatched by the 15th of the following month to the distribution list below:

| Organisation | Electronic Address for Submissions | Physical Address for Submissions | Content |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP 20, NMHB Portsmouth, PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator, Mail Point 2-4, Sir Henry Leach Building, Whale Island, Portsmouth, PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

4. **Operational Records**.

On completion of any operational activity, units are to submit PDRs/PORs/PXRs as instructed in relevant directives/exercise instructions complying with the instructions detailed in the General Instructions section of this document.

**CLASSIFICATION (to be completed)**

**MUR SUMMARY – SUBFLOT**

**UNIT:**

**MONTH & YEAR:**

**SUMMARY OF UNIT ACTIVITY:**

To include Command State, 'On' Crew, including any changes with date; operations, exercises and trails undertaken with dates and brief description; significant incidents, such as accidents or serious injuries, & major events such as VIP visits and industry days

**~~CLASSIFICATION (to be completed)~~**

DECLASSIFIED ~~UK RESTRICTED~~

CLASSIFICATION (to be completed)

**MANDATORY ENCLOSURES** **Number**

Operational reports
OSPREPS/ASSESSREPS
Weekly Sitreps
Ships Investigations
Casualty & Incident signals/reports
POLREP signals
Reports on Collisions and Groundings
Souls on Board reports
OST final assessment signals
Summary of Lessons raised to FLMS
Any other significant documents

**COMMAND COMMENTS**

Comments should include programme milestones & the unit's effectiveness against its directed tasks and during Port Visits. Command should also approve the MUR, explicitly confirming any security exclusions & identifying the custodians of these exclusions.

**SUBMISSION & DISTRIBUTION**

| ORGANISATION | ELECTRONIC ADDRESS FOR SUBMISSIONS | PHYSICAL ADDRESS FOR SUBMISSIONS | CONTENT |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP20, HMNB Portsmouth, PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator,<br>Mail Point 2-4, Sir Henry Leach Building, Whale Island, Portsmouth, PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

CLASSIFICATION (to be completed)

## ANNEX 1C

## THE FLEET AIR ARM SPECIFIC INSTRUCTIONS

1. **Application.**
This requirement applies to all Naval Air Squadrons, MASF and Flights/Detachments thereof. This replaces the need to submit Squadron and Flight Record Books to the Fleet Air Arm Museum.

2. **Narrative Requirement.**
Naval Air Squadrons are to comply with Monthly Unit Record (MUR) instructions as prescribed in the General Instructions amended as follows.

a. **UK Based Squadrons.** Squadrons that are permanently based ashore in the UK such as training Squadrons, or Squadrons with a permanently UK based headquarters elements (eg 815 NAS) are to complete MURs with associated Mandatory Enclosures.

b. **Embarked Squadrons**. Squadrons that embark en-masse are to complete MURs with associated Mandatory Enclosures. When embarked, a copy of the Squadron MUR is to be passed for inclusion with the ship's MUR.

c. **Embarked Flights.** Ship's Flights are to complete MURs with associated Mandatory enclosures. When embarked, a copy of the Flight MUR is to be passed for inclusion with the ship's MUR. This is not required for months spent disembarked but reporting should continue as part of the UK parent squadron (eg 815 NAS).

d. **Squadron Detachments/Deployments.** For detachments/deployments the CO/Detachment Commander is to ensure MURs with associated Mandatory Enclosures are completed. These MURs are to be passed for inclusion within the parent Squadron's MUR.

e. As part of the monthly submission, all Squadrons are to include the following Mandatory Enclosures with their MUR submission:

(1) Any Operational Reports submitted within the calendar month (see General Policy Principles, Para 4).

(2) Periodic Sitreps.

(3) *Flight Authorisation Sheets*. These documents are to be retained in Unit for 12 months but are to be submitted to NHB as an enclosure to the MUR exactly 12 months later. (ie: FAS Aug 10 is submitted with the MUR Aug 11).

(4) Unit Investigations.

(5) Casualty & Incident Signals/Reports.

(6) Staff List to be included when updated.

(7) Summary of Lessons raised to FLMS [See RNTM 141/07].

DECLASSIFIED
UK RESTRICTED

Additionally for all units:

(8) Any other signal or document deemed of interest or significance to the historical record of the unit.

f. **Submission & Distribution**. The MUR is to be despatched by the 15th of the following month to the distribution list below:

| Organisation | Electronic Address for Submissions | Physical Address for Submissions | Content |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP 20, NMHB Portsmouth, PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator, Mail Point 2-4, Sir Henry Leach Building, Whale Island, Portsmouth, PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

3. **Operational Records.**

On completion of any operational activity, units are to submit PDRs/PORs/PXRs as instructed in relevant directives/exercise instructions complying with the instructions detailed in the General Instructions section of this document.

**CLASSIFICATION (to be completed)**

**MUR SUMMARY – THE FLEET AIR ARM**

**UNIT**:

**MONTH & YEAR**:

**SUMMARY OF UNIT ACTIVITY:**

To include Command State, including any changes with date: operations, exercises and trails undertaken with dates and brief description; significant incidents, such as accidents or serious injuries, & major events such as VIP visits and industry days

**CLASSIFICATION (to be completed)**

DECLASSIFIED
UK RESTRICTED

DECLASSIFIED

CLASSIFICATION (to be completed)

**MANDATORY ENCLOSURES** **Number**

Operational reports
Periodic Sitreps
Flight Authorisation Sheets (-12 Months)
Unit Investigations
Casualty & Incident signals/reports
Staff List
Summary of Lessons raised to FLMS
Any other significant documents

**COMMAND COMMENTS**

Comments should include programme milestones & the unit's effectiveness against its directed tasks. Command should also approve the MUR, explicitly confirming any security exclusions & identifying the custodians of these exclusions.

**SUBMISSION & DISTRIBUTION**

| ORGANISATION | ELECTRONIC ADDRESS FOR SUBMISSIONS | PHYSICAL ADDRESS FOR SUBMISSIONS | CONTENT |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP20, HMNB Portsmouth, PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator,<br>Mail Point 2-4, Sir Henry Leach Building, Whale Island, Portsmouth, PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

CLASSIFICATION (to be completed)

DECLASSIFIED

DECLASSIFIED

## ANNEX 1D

## ROYAL MARINES SPECIFIC INSTRUCTIONS

1. **Application**.

This requirement applies to all Royal Marine units including HQ 3 Cdo Bde, UKLF CSG, 40, 42 & 45 Commandos, Cdo Log Regiment RM, FPGRM, 539 ASRM, 1 Assault Group RM, 4, 6 & 9 Assault Squadrons RM, 11 ATT Squadron RM and all RM Band Units. It also applies to independent sub-units on operations, such as Armoured Support Company (VIKING) Royal Marines. This replaces the need to submit an Annual Historical Diary to the Royal Marines Historical Officer.

2. **Royal Marine Units & Formations operating as part of a Land Component.**

RM units and formations operating as part of a land component (ie on Operations TELIC and HERRICK) are to complete the standard Army Operational Record according to the latest version of Army Form C2119. Once the C2119 is opened this replaces the MUR and this change should be noted in the final MUR summary, which should record the date that the C2119 commences. During the deployment the C2119 should be submitted to the Naval Historical Branch, as per the special instructions for Royal Marine units within the Army forms. Army units within Royal Marine formations should submit their C2119 to DG Info/ Historical Branch Army, as per the instructions within the Army forms. [Questions concerning the C2119 system should be addressed to INFO-CMEM4 /
Royal Marine units should recommence the keeping and submission of MURs on the date they close their C2119. The first MUR submission should detail the previous period C2119's were submitted in order to maintain record continuity.

3. **Narrative Requirement.**

The above units are to complete a Monthly Unit Record (MUR) with associated Mandatory Enclosures as prescribed in the General Instructions with the following specific caveats.

a. FPGRM Protection/Boarding Teams and LPD Boat Squadrons are to produce MURs for inclusion within the host ships MUR during embarked periods.

b. As part of the monthly submission, all units are to include the following Mandatory Enclosures with their MUR submission:

(1) Any Operational Reports submitted within the calendar month (see General Policy Principles, Para 4).

(2) Periodic Sitreps

(3) Any sub-unit reports (ie Boarding Teams)

(4) Unit Investigations.

(5) Casualty & Incident Signals/Reports.

(6) Staff Lists are to be included when updated.

(7) Summary of Lessons raised to FLMS [See RNTM 141/07].

Additionally for RM units and formations:

(8) Any other signal or document deemed of interest or significance to the historical record of the unit.

DECLASSIFIED

DECLASSIFIED

c. **Submission & Distribution.** The MUR is to be despatched by the 15th of the following month to the distribution list below:

| Organisation | Electronic Address for Submissions | Physical Address for Submissions | Content |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP 20, NMHB Portsmouth, PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator, Mail Point 2-4, Sir Henry Leach Building, Whale Island, Portsmouth, PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

4. **Operational Records.**
On completion of any operational activity, the Royal Marine units listed above are to submit PDRs/PORs/PXRs as instructed in relevant directives/ exercise instructions complying with the instructions detailed in the General Instructions section of this document.

**CLASSIFICATION (to be completed)**

**MUR SUMMARY – ROYAL MARINES**

**UNIT:**

**MONTH & YEAR:**

**SUMMARY OF UNIT ACTIVITY:**

To include Command State, including any changes with date; operations, exercises and trails undertaken with dates and brief description; significant incidents, such as accidents or serious injuries, & major events such as VIP visits and industry days

**CLASSIFICATION (to be completed)**

DECLASSIFIED

CLASSIFICATION (to be completed)

## MANDATORY ENCLOSURES

**Number**

Operational reports
Periodic Sitreps
Sub-unit Reports (i.e. Boarding Teams)
Unit Investigations
Casualty & Incident signals/reports
Staff List when updated
Summary of Lessons raised to FLMS
Any other significant documents

## COMMAND COMMENTS

Comments should include programme milestones & the unit's effectiveness against its directed tasks. Command should also approve the MUR, explicitly confirming any security exclusions & identifying the custodians of these exclusions.

## SUBMISSION & DISTRIBUTION

| ORGANISATION | ELECTRONIC ADDRESS FOR SUBMISSIONS | PHYSICAL ADDRESS FOR SUBMISSIONS | CONTENT |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP20, HMNB Portsmouth, PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator,<br>Mail Point 2-4, Sir Henry Leach Building, Whale Island, Portsmouth, PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

CLASSIFICATION (to be completed)

## ANNEX 1E

## BATTLESTAFFS, TASK FORCE COMMANDERS, NAVAL PARTIES & FLEET DIVING SQUADRON SPECIFIC INSTRUCTIONS

1. **Application.**
This requirement applies to all FLEET 2 and 1 Star Command Staffs, Naval Parties *and the Fleet Diving Squadron.*

2. **Narrative Requirement.**
2 Star Battlestaffs, COMATG,1 Star deployed Commanders and Fleet Diving Squadron are to complete a Monthly Unit Record (MUR) with associated Mandatory Enclosures as prescribed in the General Instructions adhering to the following additional instructions.

a. **2 Star HQs and COMATG**. These Headquarters are required to complete MURs throughout the year covering details of their activity.

b. **Deployed Commanders & Naval Parties**. Deployed Commanders (such as CTF 150, CTF 158, COMUKTG, UKMCC Bahrain & Mine Warfare Battle Staffs) and Naval Parties are to commence MUR reporting on standing up in preparation for any particular operation/exercise. The MUR is to be maintained throughout the activity and submitted to the NHB on completion.

c. **Fleet Diving Squadron**. Fleet Diving Squadron HQ is to submit a collated MUR on behalf of the Fleet Diving Groups.

d. As part of the monthly submission, Commanders are to include the following Mandatory Enclosures with their MUR submission:

(1) Any Operational Reports submitted within the calendar month (see General Policy Principles, Para 4).

(2) Periodic Reports & ASSESSREPS.

(3) Trip Reports.

(4) Unit Investigations.

(5) Casualty & Incident signals/reports.

(6) Staff Lists are to be included when updated.

(7) Summary of Lessons raised to FLMS [See RNTM 141/07].

Additionally for all Commanders:

(8) Any other signal or document deemed of interest or significance to the historical record of the unit.

e. **Submission & Distribution**. The MUR is to be despatched by the 15th of the following month to the distribution list below:

DECLASSIFIED

| Organisation | Electronic Address for Submissions | Physical Address for Submissions | Content |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP 20, NMHB Portsmouth, PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator, Mail Point 2-4, Sir Henry Leach Building, Whale Island, Portsmouth, PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

3. **Operational Records**.

On completion of any operational activity, Commanders are to submit PDRs/PORs/PXRs as instructed in relevant directives/exercise instructions complying with the instructions detailed in the General Instructions section of this document

**CLASSIFICATION (to be completed)**

**MUR SUMMARY – BATTLESTAFFS & NAVAL PARTIES**

**UNIT**:

**MONTH & YEAR**:

**SUMMARY OF UNIT ACTIVITY:**

To include Command State, including any changes with date; operations, exercises and trails undertaken with dates and brief description; significant incidents, such as accidents or serious injuries, & major events such as VIP visits and industry days

**CLASSIFICATION (to be completed)**

DECLASSIFIED

CLASSIFICATION (to be completed)

**MANDATORY ENCLOSURES** **Number**

Operational reports
Periodic Sitreps & ASSESSREPS
Trip Reports
Unit Investigations
Casualty & Incident signals/reports
Staff List when updated
Summary of Lessons raised to FLMS
Any other significant documents

**COMMAND COMMENTS**

Comments should include programme milestones & the unit's effectiveness against its directed tasks. Command should also approve the MUR, explicitly confirming any security exclusions & identifying the custodians of these exclusions.

**SUBMISSION & DISTRIBUTION**

| ORGANISATION | ELECTRONIC ADDRESS FOR SUBMISSIONS | PHYSICAL ADDRESS FOR SUBMISSIONS | CONTENT |
|---|---|---|---|
| Naval Historical Branch | CNS-NHB HS3 | The Curator, Naval Historical Branch, No. 24 Store, PP20. HMNB Portsmouth. PO1 3LU. | MUR Summary & ALL enclosures |
| Maritime Warfare Centre | FLEET-MWC LESSONS ADMIN | FLMS Administrator,<br>Mail Point 2-4, Sir Henry Leach Building, Whale Island. Portsmouth. PO2 8BY | MUR Summary & Summary of Lessons raised to FLMS |

CLASSIFICATION (to be completed)