MINISTRY OF DEFENCE

JSP 441

Defence Records Management Policy and Procedures

Version 4.2

August 2011

Chief Information Officer
Corporate Memory

TABLE OF CONTENTS

FOREWORD

About this Document

1. I am very pleased to be able to introduce JSP 441 – Defence Records Management Policy and Procedures.

2. Good records management is essential. It is fundamental to ensuring we keep and can access the information we need to do our jobs, so that we can meet Defence objectives and fulfil our obligations as a Department of State. Having good records of decisions and actions enables MOD[1] to learn from experience, to respond to challenges and to explain our actions. Good record keeping also helps us comply with the Public Records, Data Protection and Freedom of Information Acts.

3. This document 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 policy and procedures are intended to apply to all.

4. This document covers the following:

4.1. It explains our legal obligations and sets out our statutory obligations under the Public Records Acts of 1958 and 1967.

4.2. It defines the policy which applies throughout MOD, i.e. within MOD HQ, TLBs, Service formations and units and Defence Agencies. Where the regulations governing different parts of MOD vary this is made clear.

4.3. It explains how the task of managing the records we produce is co-ordinated, and identifies the roles and responsibilities of business units.

4.4. It describes how to store information so that it can be retrieved and managed effectively, and sets out efficient methods of reviewing and disposing of information.

5. Please take time to read this policy, talk about it within your business unit and think about how you can use it to improve records management within your organisation.

MOD Departmental Records Officer

Equality and Diversity

This policy has been equality and diversity impact assessed in accordance with Departmental policy. This resulted in a:

- Part 1 screening only completed (no direct discrimination or adverse impact identified). This policy is due for review in August 2014.

[1] 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.

CHAPTER 1

Background

1.1. Information created or acquired by MOD staff in the course of their work must be regarded as a Corporate Resource of the MOD. Where information is of any lasting significance, then it should be captured as a record on MOD systems. Once it has been recorded, then the record must be actively managed through its lifecycle.

1.2. Good records management is essential. It supports daily business within those organisations that create records and also the wider departmental need for information. It enables the MOD to respond to challenges and support its actions. Without it, compliance with the Public Records, Data Protection and Freedom of Information Acts is impossible.

1.3. This JSP, which aims to conform to the Code of Practice pursuant to Section 46 of the Freedom of Information Act 2000 and the requirements as laid down in BS ISO 15489 1:2001 Information and Documentation – Records Management, sets out MOD records management policy.

1.4. This JSP does not cover those Information Management policy aspects associated with document creation. These are covered in JSP 747 – Defence Information Management Policy and associated Information Management Protocols.

1.5. The setting of policy, procedures and processes for the capture and management of Single Service Key Operational Records is the responsibility of the Single Service Historical Branches. However, this policy mandates that such records must be kept. The Single Service Key Operational Records Keeping policies for the Royal Navy (including the Royal Fleet Auxiliary (RFA)), Army and Royal Air Force can be found in BR9461, LFSO1120 and AP3040 respectively. For further information regarding Single Service Key Operational Records please contact: Navy Historical Branch for the Royal Navy and Royal Marines; the Corporate Memory Analysis team for the Army, PJHQ and any other Joint Headquarters or Units; and Air Historical Branch for the Royal Air Force.

1.6. The policy and procedures for Joint Key Operational Record Keeping are contained in this JSP (Chapter 9).

1.7. Key Operational Records, which are a subset of all the information created on operations, will be selected for transfer to The National Archives for permanent preservation.

Underpinning Legislation

The Public Records Act 1958 & 1967

1.8. 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.

1.9. 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 National Archives (TNA), located at Kew, and to destroy all records which are not selected.

1.10. 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.

1.11. 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. Because of the value of the public records it holds, TNA is recognised as one of the most significant archives in the world.

1.12. It is also permissible for public records to be held in places other than TNA (known as "approved places of deposit") with the Lord Chancellor's approval.

The Freedom of Information Act 2000

1.13. 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 is released proactively though the Publication Scheme. 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. Similar statutory rights to environmental information are provided by the Environmental Information Regulations 2004 (EIRs).

1.14. The FOI Act and the EIRs provide the legislative basis for public access to records which are not held by TNA. However, it is possible to exempt information from release by application of relevant exemptions under FOI, and under EIR exceptions.

1.15. The MOD policy lead on issues relating to openness, including implementation of the FOI Act, rests with the Chief Information Officer (CIO).

1.16. Guidance on the application of the FOI Act in MOD issued by the CIO’s organisation can be found on the Defence Intranet: Respond to Requests for Information and Use the FOI Guidance. Guidance on the EIRs can be found on the Defence Intranet.[2]

1.17. 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 Data Protection Act 1998

1.18. The Data Protection Act (DPA) 1998 concerns the handling and protection of and rights of access to personal data held by any organisation whereas the FOI Act

[2] Guidance Note B3: Environmental Information Regulations 2004: http://headoffice.dii.r.mil.uk/sites/info/Info-Access/Freedom%20of%20Information/FOI%20Guidance/FOI%20Guidance%20Version%206%20May%202008/Final%20FOI%20Guidance%20Notes%20v6/B3%2020090305-MOD%20FOI%20Guidance%20Access%20to%20Information%20legislation-B3.pdf

relates to the disclosure of information held by public authorities. The DPA applies to all parts of the MOD.

1.19. Responsibility for ensuring the implementation of the DPA throughout MOD lies with the CIO. All Service and civilian members of staff are bound by its provisions, which confer certain rights and responsibilities. For more information about the implications of the DPA please refer to the DPA Defence Intranet guidance: Comply with the Data Protection Act.

What Are Public Records?

1.20. All documents generated by government departments are legally Public Records as covered by the terms of the Public Records Acts.

1.21. This does not however mean that all documents will be worthy of permanent preservation. Each department must select those documents which merit permanent preservation and safeguard them accordingly. Subsequently decisions must be made about the length of time for which records should be retained taking into account issues such as legal or contractual requirements.

1.22. Once the administrative need to retain a record has ceased a decision needs to be made on whether the record has historical value and merits permanent preservation. For the MOD this task is undertaken on behalf of CIO by the Defence Business Services Knowledge and Information (DBS KI) team, who assess the recommendations made by the originating business unit.

What should be kept as a Record?

1.23. Records contain information, created or received in the course of MOD business, and which is judged to have short- or long-term corporate value. It is the responsibility of business units, working with their TLB and Corporate Memory, to determine what has value, and to ensure that such information is retained. All records should be stored and protected for a specified retention period, thus making them readily accessible while they are still required for local or corporate use.

1.24. The information can be in any format, usually now electronic, but often on paper, and occasionally other forms. The information may be of any type – letters, emails, spreadsheets, presentations, databases, web pages, images, maps, video, audio, for example.

1.25. An aim of records management is to select and save records in such a manner that they tell the full story of activities undertaken by the department now, and will continue to do so in the future. In order to ensure that you, your team, your successors, the wider MOD and government, and possibly the general public, can access your work in the future, you must store it as a record.

1.26. There are certain types of records likely to warrant permanent preservation. Examples of these are included in this JSP and in IM Protocol 011 – What is a Record? It is particularly important that such records are created, and then managed, carefully and thoroughly.

The Importance of Records to MOD

1.27. The MOD and the Armed Services are large, heterogeneous 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 open to legal, Parliamentary, media and personal challenge, often many years after the event. Business units, whether they are the originators of the action or successors[3], need to know what happened and why.

1.28. Selection of records for medium- and long-term preservation for administrative use needs care, some 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 CIO (Corporate Memory Records).

1.29. If in doubt, err on the side of caution and forward the material to the MOD Archives 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' and IM Protocol 010 – Keeping A Record.

Risks to MOD if inadequate records are kept

1.30. Poor and inadequate records management creates risks to the MOD. These include:

1.30.1. The risk to current or future operations.

1.30.2. The risk of embarrassment to Ministers or Senior Military Officers.

1.30.3. The risk of direct or indirect financial loss.

1.30.4. The risk of impaired public confidence.

1.30.5. The risk that MOD does not comply with legislation and/or regulations or is unable to support legal proceedings.

The MOD Departmental Records Officer

1.31. 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 effective and in line with the statutory requirements of the Public Records and FOI Acts, and other relevant legislation.

1.32. However, for the MOD to effectively manage its records requires that effective support arrangements are in place with all staff aware of their clearly defined responsibilities. Details of the various records management roles and responsibilities can be found in Chapter 2.

[3] The terms 'branch or business unit" are used for convenience as a reference to each part of a Directorate or Service formation which maintains a discrete file plan and which is responsible for the opening, closing, review and disposal of files. Civilian ranks are also used for convenience and should be taken to equate to their Service equivalent where appropriate.

CHAPTER 2

Records Management Role and Responsibilities

MOD Departmental Records Officer

2.1. 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 to ensure that departmental business is effective and in line with the statutory requirements of the Public Records and Freedom of Information (FOI) Acts, and other relevant legislation.

2.2. The MOD DRO is the Head of Corporate Information (CI) within the Chief Information Officer's (CIO) organisation, on whose behalf day to day responsibility is discharged by Corporate Memory. The DRO is accountable for MOD's records stored in both the sensitive archive at HM Naval Base, Portsmouth and the main archive run by TNT on behalf of the Department at Swadlincote, Derbyshire; and the review and transfer of selected records to TNA. The DRO is responsible for:

2.2.1. 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.

2.2.2. MOD's selection policy to determine whether records merit permanent preservation.

2.2.3. The records management advisory service provided to Information Hubs (iHubs).

Corporate Memory Records

2.3. The Corporate Memory Records team is responsible for:

2.3.1. Developing and promulgating MOD's records management policy through the publication of JSP 441 (Defence Records Management Policy and Procedures).

2.3.2. Providing expert advice and guidance on records management and raising the profile and awareness of records management across the MOD.

2.3.3. The development of a maturity model and associated self-assessment toolkit that will govern the regular collection and promulgation of MOD records management statistics and will be used to assess the standard of records management in Defence.

2.3.4. Developing and conducting a programme of Information Management Assessments and other assurance activities to measure and improve record keeping standards and processes across the MOD.

2.3.5. Ensuring that records management is included in the appropriate training packages.

2.3.6. Determining the MOD's future records management strategy and as such contributes to the development of the Defence Information Infrastructure electronic records management solution and the MOD strategy for the long-term management and preservation of digital information.

2.4. The Corporate Memory Records Team can be contacted at:

- Room 3.G
- MOD Main Building
- Whitehall, London,
- SW1A 2HB
- Email: cio-ci-cmemrecordsgroupmailbox@mod.uk
- Telephone (Mil): 9621 84405 or 9621 82871 or 9621 80132

DBS KI Contract Management Team

2.5. The Defence Business Services Knowledge and Information (DBS KI) Contract Management Team (CMT) is responsible for managing day-to-day issues relating to the MOD’s paper files held at TNT Archive Services at Swadlincote in Derbyshire. The archives house most of the records up to SECRET in registered files along with unregistered records, a large quantity of service and civilian personnel records, and scientific and technical material. The 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.

2.6. The Contract Management Team can be contacted on:

- Telephone (Mil): 94240 5701

DBS KI Records and Review Team

2.7. The DBS KI Records and Review team is responsible for:

2.7.1. The archive in Portsmouth that houses TOP SECRET and other sensitive material, and 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 twenty five years after their last recorded action. It is through this process, incorporating the recommendation made by the originating business unit, that records worthy of permanent preservation are selected. These selected records are prepared by the team for transfer to The National Archives (TNA).

2.7.2. Historical information, defined as information that is over twenty five years old, only. Material stored in the MOD Main Archive or in the MOD Sensitive Archive which is less than twenty five years old is the responsibility of the originating branch or its successor organisation.

2.7.3. Responding to FOI requests for records over twenty five years.

2.8. The Records and Review team can be contacted on:

- Telephone (Mil): 9380 25215 or 9380 25217

Other Records Management Roles

2.9. For the MOD to effectively manage its records requires that effective support arrangements are in place with all staff aware of their clearly defined responsibilities.

Senior Information Officer

2.10. Each organisation and deployed HQ is responsible for the maintenance of the records it generates or receives, and the material it stores in the MOD Main Archive or the MOD Sensitive Archive which is less than twenty five years old, and as such must nominate a Senior Information Officer (SIO) who:

2.10.1. Owns the information within the organisation.

2.10.2. Is accountable for the quality and provenance of the information produced.

2.10.3. Sets local records management policy and culture.

2.10.4. Appoints an Information Manager (IMgr) who ensures that effective records management procedures are put in place and maintained and is responsible for managing the information flow and enforcing information and records management activities on behalf of the SIO.

2.11. The SIO is to ensure that full contact details for the IMgr are forwarded to the Corporate Memory Records team and that these are updated to reflect any subsequent change. The records management responsibilities of the SIO include ensuring that:

2.11.1. All business unit file plans have been approved by Corporate Memory Records team. Each file plan is to be accompanied by a retention schedule.

2.11.2. 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 440: The Defence Manual of Security and JSP 441 and are to be issued throughout the organisation.

2.11.3. Suitable monitoring arrangements are in place to ensure that records management procedures are embedded and maintained. If the SIO determines that there is a major weakness in the existing records management procedures within the business unit it may be appropriate to recommend that a suitable change objective be incorporated into the Management Plan.

2.11.4. IMgrs have suitable procedures in place to ensure that all new Information Support Officers receive any required records management training.

Information Manager

2.12. The Information Manager (IMgr) will be the prime point of contact with the Corporate Memory Records team and will be responsible for co-ordinating the activities of subordinate Information Support Officers.

2.13. IMgrs are responsible for ensuring that the procedures outlined in this JSP and any subsequent local instructions are adhered to. Their main records management duties include:

2.13.1. The creation and continuous maintenance of the business unit file plan and retention schedule.

2.13.2. The creation and maintenance of a definitive ‘Record of Unregistered Material’ held by the business unit. This unregistered material (records not on registered files) might include maps, plans, drawings, and charts.

2.13.3. Ensuring that local records management instructions to augment those contained in JSP 441 are adhered to.

2.13.4. Coordinating the efficient and timely review of registered files (and material held other than on such files) and ensuring that this review is carried out in accordance with the instruction issued in this JSP.

2.13.5. Ensuring that Information Support Officers are given appropriate training upon their arrival.

Information Support Officer

2.14. The Information Support Officer (ISO) performs the day to day records management duties. The ISO would normally run an iHub or registry and hence has day-to-day responsibility for:

2.14.1. 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 instructions.

2.14.2. The ongoing maintenance of the business unit file plan.

2.14.3. The closure of registered files in accordance with this JSP.

2.14.4. The preparation of business unit records for disposal in accordance with the retention schedule.

2.14.5. The maintenance of a system to record the whereabouts of registered files which have been removed temporarily from their permanent location within the business unit.

2.14.6. Ensuring that ongoing records management training is provided to the business unit.

2.14.7. The supervision of other administrative support staff, for example Information Support Administrators (ISA).

Unit Personnel

2.15. Unit personnel raising or receiving official correspondence have a responsibility to:

2.15.1. Ensure that records are placed in the appropriate registered file or electronic folder.

2.15.2. Liaise with their IMgr / ISO when requesting the creation of a new registered file or folder.

2.15.3. Be involved in the review process and ultimately confirm or amend the disposal recommendation made in the business unit retention schedule.

More Information

2.16. For more information on the role of the SIO, IMgr, ISO and ISA please refer to IM Protocol 013 – IM Professional Roles.

CHAPTER 3

Records Management Policy

Introduction

3.1. Records should provide evidence of the activities that took place, establish exactly what happened and enable others to understand why decisions were taken. It is vital that records are seen to be trustworthy. 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 records management practice will ensure that through time records:

3.1.1. Are present.

3.1.2. Can be accessed by those entitled.

3.1.3. Can be understood.

3.1.4. Can be trusted (as being authentic).

3.1.5. Can be disposed of when no longer required.

3.2. All business units are to have in place an adequate system for documenting their activities which takes into account the business, legislative and regulatory environments in which they work. This system is to ensure that the record of activity is complete and accurate.

3.3. 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 is not to be amended, and is to be managed in a suitable environment to support its preservation.

3.4. A records management system supports the preservation of the records generated and used by a business unit, for as long as necessary but no longer. The Electronic Records Management System (ERMS) or registered filing system is the definitive record of business unit activity on any given subject and it is imperative that anyone using a registered file or folder can be confident that the information it contains is complete and up-to-date. It is important therefore to ensure that material which is deemed worthy of retention is declared a record as soon as possible.

3.5. The underlying principle is that staff must ensure that they maintain a proper record of business by filing or declaring all relevant information, including e-mails, electronic documents, etc. as records in their ERMS or registered files as appropriate. Where business units operate an ERMS and have material deemed worthy of retention which is not able to be captured directly into the ERMS for example physical material, this material is to be stored in a registered file and the ERMS used to track it. If this is not possible or practical business units should follow the Non-DII system Record Management Appraisal and Implementation process (see Chapter 4).

3.6. Not all records can be placed in registered files. These records may be in a range of other forms such as maps, plans, drawings, charts, video, film, photographs, technical reports, battle planners, etc. Additional guidance on these unregistered records is given in Chapters 5, 6, 7 and 8.

Records Created On Operations

3.7. There are two categories of records/information created on operations:

3.7.1. **Operational Information**: This is all the information and records created on operations, including Key Operational Records (see below).

3.7.2. **Key Operational Records**: These are high value records. They are a subset of Operational Information and are defined by the Single Service Key Operational Record Keeping policies. They provide a body of information that can be used by the Historical Branches for historical operational analysis to support MOD decision making, the development of operational capability and lessons processes as well as providing a basis for much of the record required to assist legal activity involving the Department. They are also the records of operations that MOD will transfer to The National Archives for permanent preservation.

3.8. Units and Formations must maintain a record of their activities whilst deployed on operations (including Operations in the UK), this includes the Key Operational Record and any other records it judges it needs to keep in order to discharge its duties or account for its actions. This record assists with a wide range of MOD activity from the validation of war pension claims to the compilation of official histories. It provides:

- Information to support current and future operations;
- Evidence of actions and decisions which may later be the object of disciplinary investigation; and
- Protection to Units and Commanding Officers against litigation.

3.9. All operational information created in overseas theatres must be returned to UK, stored as a record in an archive for 15 years from the date it was created and then destroyed, unless there are outstanding legal proceedings relating to the records, in which case the records will be kept until all legal proceedings have ended. Such information should be treated as a Departmental record and must be managed in accordance with the policies described in this JSP.

3.10. Once national security or personal sensitivities no longer apply, the Single Service and Joint Unit Key Operational Records will be transferred to The National Archives for permanent preservation. This process is managed by the Single Service Historical Branches.

3.11. In conjunction with the creating unit or formation the Single Service Historical Branches are responsible for the management and resolution of information requests relating to the Key Operational Records they hold. Where a unit or formation no longer exists or was temporary for the duration of an operation the Historical Branch holding the record is responsible for the Key Operational Record and should consult the force generating headquarters or its successor or parent organisation as necessary. Operational Information that has been returned from overseas Theatres and archived as a record remains the responsibility of the creating unit or formation. Where the creating unit or formation no longer exists or was temporary for the duration of the operation, responsibility for the archived record lies with the force generating headquarters or its successor or parent organisation as necessary.

Records Capture and Declaration

3.12. Capture is the process of determining that a record should be made and kept (including information both created and received by the MOD), determining who has access to the record and how long the record is to be retained. Business units are to ensure that users have a clear understanding of the information that should be captured as a record. Chapter 7 – Annex A – Appendix 1 gives examples of records likely to warrant permanent preservation.

3.13. Ephemeral documents, 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. Such documents should be destroyed when no longer needed.

3.14. The act of declaring the record provides evidence that it has been created or captured and involves recording brief descriptive information (metadata) about the record and assigning it with a unique identifier or enclosure number.

Policy

The MOD will provide a records management environment where:

- All current and newly created records is captured, stored and properly managed through time.
- Material deemed worthy of retention is declared as a record as soon as possible.
- Single Service and Joint Key Operational Records will be selected for permanent preservation.
- The Single Service Historical Branches will administer the capture and subsequent management of Key Operational Records.

The UK based headquarters responsible for an overseas operation **MUST** ensure that:

- All information created in theatre is returned to the UK and stored as a record in an appropriate archive.

The owner of the archive holding records created in theatre and returned to the UK **MUST** ensure that:

- The records are managed in accordance with JSP441.

Information Managers **MUST** ensure that:

- Where an ERMS has been implemented and they have material that is not able to be captured directly into the ERMS that this material is filed in physical registered files and the ERMS used to track it, or they follow the Non-DII system Record Management Appraisal and Implementation process.

Developers of operationally deployable IT systems **MUST** ensure that:

- They have implemented an archiving capability for the IT system and have agreed with Corporate Memory Records that it is an acceptable solution.

Classification of Records

Introduction

3.15. Classification is the process of identifying the types of activity undertaken by a business unit and the records they generate. Classification is a means of grouping “like kind” information together to facilitate description, access control and final disposal. In MOD terms a classification scheme is another name for a file plan. A file plan provides many benefits and adopting one means that it is easier to:

3.15.1. Obtain a continuous record of activity.

3.15.2. Retrieve all records relating to a particular function, topic or activity.

3.15.3. Achieve security and manage access.

3.15.4. Manage retention and disposition.

File Plans

3.16. File plans define a hierarchical filing structure into which individual records are filed. A good file plan should be intuitive and should simplify the task of deciding where to declare a particular record. Since it is impracticable to review high volumes of records individually, a file plan will also assist the decisions regarding the review, retention and disposal of folders.

3.17. The structure of a file plan to be used for managing records is to closely follow the guidance described in Chapter 4 for electronic records and Chapter 5 for physical records.

Retention Schedules

3.18. Retention schedules are an essential aspect for all records management systems. They document how long records will be retained and ensure that folders and registered files[4] are reviewed (usually after a period of years) to determine the appropriate disposal action to be taken on each folder (see Chapter 7). Appropriate retention schedules must be applied to every folder and registered file in the file plan hierarchy.

File Plan Approval

3.19. Whilst many of the records MOD creates will eventually be deleted, some will require long-term retention for corporate use, and may ultimately be worthy of permanent preservation at The National Archives (TNA).

[4] The ‘owner’ of a folder or registered file should be of a grade of at least Band C2 or equivalent. The owner or Reviewing Officer will be responsible for performing the review and determining the final disposal of the folder or registered file.

3.20. To make an early determination of these potentially valuable records, the Corporate Memory Records team (see Chapter 2 for contact details) will review and approve all file plans and retention schedules to identify “key” folders and registered files that are likely to contain records that have long-term value or are worthy of permanent preservation. Once these “key” folders and registered files have been identified, although they continue to be managed and accessed by their respective business unit(s) for as long as they are needed locally, the Corporate Memory Records team will be responsible for determining the disposal or retention periods to be applied to these records after any review process.

Policy

The MOD will provide a records management environment where:

- A complete and accurate record of business activity can be kept.

The Information Manager **MUST** ensure that:

- The business unit operates and maintains a classification scheme or file plan.
- A single file plan is used for all records held or tracked by the business unit irrespective of the media (for example electronic, paper, optical, film) on which they are held.
- Only iHub staff can create and maintain the file plan. (I.e. no other personnel are to create electronic classes and/or folders and folder parts or physical registered files.)
- A unique file number reference is applied to each registered file in the physical environment. (A unique folder number reference may be applied to each class and folder in the electronic environment.)
- Each class and folder in the electronic environment or registered file in the physical environment must bear an approved retention schedule.
- The file plan structure, i.e. main headings, folder/file numbers and associated retention schedules of all business unit file plans are approved by the Corporate Memory Records team before use.
- Newly opened electronic folders have relevant metadata associated with them. See Chapter 4 for more details.
- An owner has been assigned to every new folder or registered file to assist with the eventual review and disposal.
- Business unit personnel store their records in folders or registered files in the appropriate ERMS and/or registered file system.

Access to Records

Introduction

3.21. JSP 440: The Defence Manual of Security describes the guidelines regulating who is permitted access to records and in what circumstances. Records may contain personal, commercial or operationally sensitive information and in some cases access to these records, or even information about them, should not be permitted to everyone. The records management system should provide timely and efficient access to, and retrieval of, those records required by users with the relevant permissions in the course of their business.

3.22. All MOD personnel are required to share information responsibly and sensibly. Sensitive records about individuals and records that are protectively marked are to be labelled accordingly and access limited to those who genuinely need them to perform their duty. See JSP 747: Defence Information Management Policy and Protocols and JSP 440 for more details. Failure to adhere to these policies may lead to disciplinary proceedings.

3.23. All MOD personnel should also be aware of their responsibilities as laid down in the Official Secrets Act. In short, it is an offence for anyone to disclose official information where it would be reasonable to expect it to be protected by the Act. See JSP 440 Part 9, Chapter 2, for more details.

3.24. MOD will ensure that electronic records are accessible and usable for as long as they are needed, and that the risks of technological obsolescence are addressed. This will be achieved by implementing processes and solutions in accordance with TNA technical standards and guidance.

Off line Storage

3.25. The decision to capture a record implies an intention to store it ensuring that it is protected, accessible and properly managed throughout its lifetime. Material deemed worthy of retention, therefore, needs to be stored in an environment conducive to its long-term preservation.

3.26. Electronic records are not to be maintained solely offline (for example on CDs, DVDs etc.) without prior consultation with Corporate Memory, as this makes them difficult for users to discover or access, and risks them becoming inaccessible due to media obsolescence.

Misfiled Records

3.27. Records are not to be transferred between electronic folders or registered files unless they have been misfiled. All record transfers of this type are to have an audit log that details the name of the individual who performed the transfer, the date of transfer, the record reference and the identities of the source and destination files.

Cryptography

3.28. Definitive guidance on cryptography is available in JSP 440 and JSP 602: 1032 - Cryptography and Key Management.

3.29. 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. Therefore, encrypted records are not to be declared into an ERMS. They are to be declared in their unencrypted form.

Digital Signatures

3.30. 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 the original author, the signature will no longer be valid when cryptographically checked. A digitally signed document can be stored in an ERMS but it is to be in its native unencrypted (clear text) format.

Self Modifying Fields

3.31. Electronic records with self modifying fields, for example a date field that automatically updates to reflect real or current time, will not display correct information when the record is viewed in future. If users declare records that contain self modifying fields, then the integrity of the record may be compromised. These fields are to be made permanent prior to declaration.

Reference Material

3.32. Any information referenced within a record (for example 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. For reference material that is impractical to file, this material is to be tracked by the ERMS or the physical records management system.

3.33. If you make decisions based on third 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.

Policy

The MOD will provide a records management environment where:

- Records can be stored in a format that allows continued access for the duration of the records lifecycle.

Information Managers **MUST** ensure that:

- The highest security protective marking of the content of any registered file is clearly identified.
- Corporate Memory is consulted as soon as possible if any registered files are found to be missing.
- Records are managed within the creating business unit for the duration of their lifecycle, unless otherwise agreed by Corporate Memory.
- Records are only transferred between folders or registered files if they have been misfiled.

Users **MUST** ensure that:

- They share information responsibly and sensibly but where appropriate, access to records is strictly limited to those who need them to perform their duty.
- Access permissions are not applied to individual records. These permissions must be set and/or placed on the medium in which the records are stored.
- Electronic records declared to the ERMS are not encrypted, compressed, password protected, etc. to ensure that they remain accessible for as long as required. They must be declared in their decompressed or unencrypted form.
- Digitised signatures, which are digitised representations of an individual's own hand written signature, are not to be used as they may give a document a spurious authority and are an invitation to fraud.
- Electronic records are not stored offline. The use of offline media such as CD and DVD for the storage of electronic records is prohibited.
- Self modifying fields within an electronic record are made permanent prior to declaration into the ERMS.

Records Disposal[5]

Introduction

3.34. Good records management practice ensures that through time, records can be disposed[6] of when no longer required. From this two important questions need to be addressed: How long do we keep the records we have stored and what do we do with those records we no longer have to keep?

3.35. Answering these questions will depend on the nature of the records and is addressed in part by applying appropriate retention schedules to file plans. The policy statements below outline the processes individuals are to follow before a folder is closed and the actions that are to take place after the folder has been closed and its associated retention schedule implemented.

Key Folders/Registered Files

3.36. Within business unit file plans, the Corporate Memory Records team will earmark any folders or registered files that are of specific long-term interest at departmental level as ‘key’. These “key” folders / registered files will fall under Corporate Memory ownership, but the business unit will continue to manage and access the records for as long as they are needed locally.

Closing Folders

3.37. To aid cross-departmental thematic review, and allow related records held on different systems (for example at different levels of protective marking) to be linked, electronic folders (parts) are to be closed on an annual basis, with new parts created should there be a continuing business need.

3.38. IHub staff may wish to consider closing the registered file or folder altogether if it seems likely that it has no further value.

Weeding of Folders

3.39. The weeding of ERMS folders or registered files or folders is **prohibited**. One of the reasons for this is that the process of weeding files is a time-consuming and therefore costly activity. A second reason is that to ensure that preserved documents retain their original context, TNA requires MOD to select complete files for permanent preservation rather than extracts from files.

Metadata

3.40. Folder level metadata[7] is to 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 Data Protection Act (DPA) and Freedom of Information (FOI) legislation.

[5] Disposal is the review or appraisal of records to determine their long-term value and the subsequent actions (archiving or destruction) when the records are no longer needed for the conduct of the current business.

[6] For the purposes of this JSP, ‘Export’ is one aspect of disposal and is defined as the act of transferring or moving records or / and folders from one system to another.

[7] In the electronic environment, folder level metadata can be captured automatically by the ERM audit trail. MOD Form 262F is the physical equivalent. This form, normally retained in a binder, must be kept for a minimum of 30 years following the insertion of the final MOD Form 262F.

3.41. Chapter 4 describes the minimum metadata for all classes, folders and folder parts in a file plan. Information Management staff are to ensure that this is applied at the point of creation.

Policy

The MOD will provide a records management environment where:

- Records selected for permanent preservation will be transferred to TNA (or the appropriate Place of Deposit).
- Records can be disposed of as soon as they cease to be of business use.

Information Managers **MUST** ensure that:

- Corporate Memory Records DepHd (see Chapter 2) is consulted before any folders/registered files are transferred to another MOD business unit or Government department, for example due to a Machinery of Government Change.
- Electronic records are not exported from an ERMS without prior authorisation from Corporate Memory.
- Folders / registered files are closed on a regular basis. There are a number of factors which need to be assessed when determining whether to close a folder. If any of the following criteria are met, then the folder (part) must be closed:
    - The folder contains 100 enclosures;
    - Annually on 31 December (for Electronic folders);
    - The folder has been open for 5 years;
    - The physical folder is 1 inch thick;
    - Nothing has been added to the folder for the last year;
    - Action on the subject covered by the folder has come to an end.
- A new folder part is not opened unless there is likely to be an imminent need to declare new records.
- When a folder part is closed, appropriate metadata is captured.
- A regular review of the contents of closed folder parts takes place.
- Local review and disposal of records is not carried out on the contents of “key” folders. IHub staff must liaise with the Corporate Memory Records team regarding any disposal action.
- The ‘weeding’ of ERMS folders / registered files does not occur. The ‘weeding’ of folders is prohibited.
- Folder level metadata is retained after a folder part has been destroyed, for a minimum period of 30 years.

Chapter 3 – Annex A

TOP SECRET, STRAP and Codeword Records

3A.1. All MOD personnel are required to share information responsibly and sensibly. JSP 440: The Defence Manual of Security describes who is permitted access to records and in what circumstances. Records may contain personal, commercial or operationally sensitive information and in some cases access to these records, or even information about them, should not be permitted to everyone.

3A.2. Sensitive records about individuals and records that are protectively marked are to be labelled accordingly and access limited to those who genuinely need them to perform their duty. See JSP 440 and JSP 747: Defence Information Management Policy and Protocols for more details. Failure to adhere to these policies may lead to disciplinary proceedings.

3A.3. The policy for all imagery that the UK collects or receives for intelligence purposes, or which is deemed to be of intelligence value: this includes satellite imaging systems (military and commercial) and airborne, ground-based and sea-borne collection systems can be found in JSP 348 - UK Defence Imagery Policy: Regulations For Demanding, Storage, Archive, Retrieval And Imagery Training.

3A.4. All MOD personnel should also be aware of their responsibilities as laid down in the Official Secrets Act. In short, it is an offence for anyone to disclose official information where it would be reasonable to expect it to be protected by the Act. See JSP 440 Part 9, Chapter 2 for more details.

3A.5. The definition of the TOP SECRET protective marking, and instructions for maintaining, sending and receiving such material, are contained within JSP 440 Part 5, Chapter 1.

Specific Policy

3A.6. Intelligence and Security Agency End Product[8] **MUST NOT** be declared as a MOD record, and will be retained by the originating Agency in accordance with their records management policies.

Electronic Records Management

3A.7. Until an ERMS is available on MOD TOP SECRET systems, electronic records protectively marked as TOP SECRET and above must be printed out, filed in registered files and managed in accordance with the guidance contained in Chapter 5 unless alternative arrangements have been agreed with CIO-CI-Corporate Memory Records DepHd.

3A.8. Foreign owned or Agency TOP SECRET, STRAP equivalent, and/or codeword material will not be transferred to TNA. There is, therefore, no requirement to print this material unless there is no other way to access it for business purposes.

3A.9. When an ERMS is available to handle TOP SECRET material, the ERMS is to comply with the requirements as laid down in Chapter 4, Parts 1 and 3. In addition

[8] End Product covers any reporting created on Agency End Product publishing systems (i.e. any reporting for wider distribution, as distinct from items held on their corporate systems and intended for internal consumption only).

to these requirements, a mechanism must exist to allow the DBS KI Records Review team access to all electronic records – including codeword and image records – that are aged 25 years or older.

Paper and Non Digital Imagery Records

3A.10. TOP SECRET, STRAP and codeword material **MUST NOT** be sent to TNT Archive Services. Such material **MUST** be sent to the Sensitive Archive in accordance with the guidance described in Chapter 8 Annex A.

3A.11. Non digital imagery selected for preservation, but which still merits a TOP SECRET protective marking, **MUST** be forwarded to the DBS KI Records Review team for storage in the appropriate archives. There is no requirement to forward foreign owned or Agency imagery material to the MOD Archives.

3A.12. Business units **MUST NOT** forward TOP SECRET imagery to the DBS KI Records Review team without prior consultation with them. When agreement is given, the material must be sent, in accordance with appropriate JSP 440 Part 5, Section 3 procedures, to the DBS KI Records Review team. See Chapter 6 Annex B for further details.

Review and Disposal of Records

3A.13. As TOP SECRET, STRAP and/or codeword material approach the end of their retention schedule, the business unit must review them and determine whether the material should be retained for business purposes, considered for permanent preservation or destroyed.

3A.14. The specific enclosures which justify an extended retention or permanent preservation recommendation (which should also be identified on the file minute sheet) should be recorded on the MOD Form 262F or within the ERMS. If there are a large number of enclosures which justify such a recommendation only the key enclosures need be identified.

3A.15. The DBS KI Records Review team is then to be given access to the material together with the business unit's recommendation.

3A.16. Where the business unit has a requirement to retain records locally beyond the 30-year limit set by the Public Records Act 1958, the MOD must submit an application through CIO-CI-Corporate Memory Records DepHd to the Lord Chancellor's Advisory Council.

3A.17. All closed registered files containing TOP SECRET, STRAP and/or codeword material are to be forwarded to the DBS KI Records Review team, even if the Registered File Disposal Form (MOD Form 262F) recommends that the file should be destroyed.

3A.18. The review and disposal of the file will be carried out by the DBS KI Records Review team in accordance with JSP 440 Part 5, Section 6: Destruction of Protectively Marked Information.

CHAPTER 4

The MOD Filing System – Electronic Records

Introduction

4.1. This chapter addresses the policy and practice for the management of electronic records in the MOD. The policy is applicable to all existing and future electronic record collections in the MOD and covers records containing any type of information held within MOD and at all levels of sensitivity. This policy addresses:

4.1.1. 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.

4.1.2. The requirements for electronic records systems, and the processes required to ensure the quality and reliability of records as a valuable corporate information resource.

4.2. This chapter is split into 3 parts:

4.2.1. Part 1 sets out MOD Electronic Records Management (ERM) Policy and corresponding guidance for those business units using a formal Electronic Records Management System (ERMS).

4.2.2. Part 2 deals with policy and guidance for users without an ERMS capability approved by The National Archives (TNA). It also provides guidance on how to deal with electronic records on those systems[9] that will not be implemented on the Defence Information Infrastructure (DII).

4.2.3. Part 3 provides instruction to those project management teams introducing ERMS in business units where DII will not be rolled out.

Further Guidance

4.3. 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 Information Hub (iHub) for more information.

4.4. Website owners must contact the Defence Internet Team prior to closing websites in order for them to be archived by TNA.

4.5. The Corporate Memory Records team 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 Corporate Memory.

[9] In this context the term ‘system’ is used to mean any aggregation of electronic information which is, or which should be, regarded as a formal record of the MOD.

The File Plan

4.6. The ERMS file plan should define a hierarchical filing structure into which individual records are filed. The file plan must be constructed using classes and folders as this will then assist the decisions regarding the review, retention and disposal of folders.

4.6.1. A class can contain other classes or folders but not both, and never records.

4.6.2. A folder consists of folder parts that may only contain records or physical markers (no sub-folders) and is always at the lowest level of the file plan.

4.7. A single file plan must be used for all records held in, or tracked by the ERMS irrespective of the media (for example electronic, paper, optical, film) on which they are held.

4.8. File plans must be created by the business unit iHub staff following the guidance described in Chapter 4 Annex A.

4.9. IHub staff must be the only ones able to open a new electronic class, folder or folder part.

4.10. The Corporate Memory Records team may earmark sections of the file plan that are of specific long-term interest at departmental level as “key”. These “key” sections will fall under Corporate Memory ownership but the business unit will continue to manage and access the records for as long as they are needed locally. IHub staff must not modify the contents of a “key” folder part once it has closed to allow for DBS KI (see Chapter 2) review.

Opening an Electronic Folder

4.11. Electronic folders provide an identifying label under which records of a similar subject matter can be grouped together and which distinguishes separate groups of records from each other. They also enable the management of a group of records as a whole so that they can be retained, reviewed and disposed of as a consistent group.

4.12. Electronic folders enable access to a group of records as a whole and can demonstrate the narrative context in which records should be understood.

4.13. They can also be used to link together conventional paper and electronic filing environments and are an essential element in providing a single hybrid container where electronic and paper records can be held.

Considerations

4.14. A folder must not be opened until there is an enclosure to be placed in it.

4.15. The folder title and designated file number (if used) must be described clearly.

4.16. An owner must be assigned to every new folder. This is to assist with the eventual disposal of the folder.

4.17. The class and folder hierarchy must have a retention schedule associated with it that has been approved by the Corporate Memory Records team. The approved retention schedules for electronic folders are:

4.17.1. Review electronic folder either: 1 year, 7 years, 15 years or 25 years after the folder has closed.

4.18. It should be noted that where the defined retention schedule is too short, Corporate Memory reserves the authority to override any local decisions.

4.19. At least one definition from the Defence taxonomy must be applied to the folder.

4.20. The folder must be set to automatically create new parts.

4.21. The folder part must be set to close after 100 enclosures.

4.22. The folder part must be set to close on 31 December at 23:59 every year. 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.

Declaring Records into Electronic Folders

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

4.24. In instances where it is impossible to declare an item, for example a book which is perhaps too awkward or bulky to scan, the item is to be filed in a registered file and the processes described in Chapter 5 are to be followed. However, this item must be tracked using the ERMS. When the electronic folder is closed and a review of the folder is required, the item(s) on the registered file is to be passed to the "owner" for appropriate review action.

4.25. The protective marking of the electronic folder is to be the same as the highest protective marking of its contents. For example, a folder may contain a majority of CONFIDENTIAL information and only one SECRET document. This folder will be classed as SECRET. Should a RESTRICTED file exist and a new document protectively marked as "CONFIDENTIAL" or above need to be placed on it, an electronic folder in the SECRET domain is to be opened.

Contents of an Electronic Folder

4.26. Material deemed worthy of retention must be declared in an electronic folder. Guidance on the type of records deemed worthy of retention and hence, should be declared into the ERMS is given in Chapter 7 Annex A.

4.27. All records declared in to the ERMS must comply with the Document and Records Naming Protocol as described in JSP 747: Information Management Policy and Protocols.

4.28. Ephemeral documents, rough drafts, spare copies etc. need not be placed in these folders if they are likely to be needed only temporarily and are not of any lasting significance. Such documents are to be destroyed when no longer needed.

Misfiled Records

4.29. When a record has been misfiled the user must inform iHub staff who will perform the correction. The reason for and details of the user requesting the record transfer must be recorded in the ERMS.

TOP SECRET Records

4.30. Until an ERMS is available on DII (TOP SECRET), electronic records protectively marked as TOP SECRET and above must be printed out, filed in registered files and managed in accordance with the guidance contained in Chapter 5, unless separate arrangements have been agreed with Corporate Memory Records.

4.31. The instruction for maintaining, sending and receiving protectively marked material is contained within JSP 440: The Defence Manual of Security.

Material NOT stored in Electronic Folders

4.32. Not all records can be stored in the ERMS. These records may be in a range of formats including maps, plans, drawings, charts, video, film, photographs, etc. Additional guidance is given in Chapters 5, 6, 7 and 8.

Access to Electronic Records

4.33. All MOD personnel are required to share information responsibly and sensibly. Sensitive records about individuals and records that are protectively marked must be labelled accordingly and access limited to those who genuinely need them to perform their duty. Failure to adhere to ‘need to know’ guidelines may lead to disciplinary proceedings.

4.34. All MOD personnel must be aware of their responsibilities as laid down in the Official Secrets Act. In short, it is an offence for anyone to disclose official information where it would be reasonable to expect it to be protected by the Act. See JSP 440 Part 9, Chapter 2, for more details.

Transfer of Registered Files to another Government Department or MOD Business Unit

4.35. If the need arises to transfer an electronic folder, series of electronic folders or an entire file plan permanently to another government department, Corporate Memory Records DepHd (see Chapter 2) must be consulted before any transfer action is taken.

4.36. The need may arise to transfer a single/or series of electronic folders 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 Corporate Memory must be advised in writing before action is taken.

4.37. If parts of a file plan are being permanently transferred to a new business unit, the relevant electronic folders should be closed and forwarded to the "importing" business unit which will open appropriate folders, allocate new reference numbers and apply appropriate retention schedules.

4.38. Electronic folders must not be renamed.

4.39. Electronic folders must not be renumbered. If there is a need to allocate a new reference number, the folder must be permanently closed and a new folder opened. The folders should then be cross-referenced.

4.40. The "exporting" business unit must notify Corporate Memory Records DepHd in writing of the transfer and formally record the transfer of the folders and all the related but previously closed folder parts, in their file plan.

Closing a Electronic Folder

4.41. There are a number of factors which need to be assessed when determining whether to close an electronic folder part. If any of the following criteria apply, the folder must be closed:

4.41.1. The folder part contains 100 enclosures;

4.41.2. Nothing has been added to the folder for the last year (close the entire folder unless there is a clear indication that records will be added to it shortly);

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

4.42. If the actions described above for ‘Opening an Electronic Folder’ were taken, the folder part will close automatically at year end or once the number of records in the folder reached 100. However, iHub staff must monitor the file plan on a regular basis to determine whether open folders are still appropriate to the business. If after consultation with the folder owner they are deemed as no longer appropriate, these folders should be closed manually.

Reviewing Closed Electronic Folders

4.43. IHub staff must monitor closed folders on a monthly basis to ensure that folders are reviewed on schedule. Chapter 7 provides guidance on the review process.

“Weeding” of ERMS Folders

4.44. The weeding of ERMS folders is **prohibited**. One of the reasons for this is that the process of weeding folders is a time-consuming and therefore costly activity. A second reason is that to ensure that preserved documents retain their original context, TNA requires MOD to select complete folders for permanent preservation rather than extracts from folders.

Actions Following the Review of Electronic Folders

4.45. Following the review of the electronic folder, the iHub is to perform the appropriate disposal action as determined by the Reviewing Officer. This action may be to extend the period that the folder is kept in the business unit; retain it for permanent preservation, in which case ownership should be passed to Corporate Memory; or destroy.

4.46. IHub staff must not destroy any electronic folders that have been previously identified as “key” folders by the Corporate Memory Records team.

4.47. Before taking the disposal action, the iHub staff must always note the decision made by the Reviewing Officer in the ERMS. If used, iHub staff should declare the completed Electronic Folder Review Form in Chapter 7 Annex C, into an appropriate electronic folder in the ERMS. This folder should have a retention schedule of 25 years applied to it since the form will need to be kept for 30 years. This form also acts as an audit trail for the iHub staff should there be a query on the location of the folder.

4.48. If a business unit is disbanded, the folder containing the forms should be passed to the successor or parent business unit. If there is no successor or parent business unit then contact the Corporate Memory Records team immediately for advice.

Part 2 – Policy and Guidance for Electronic Record Keeping in the Absence of an Electronic Records Management System (ERMS)

Introduction

4.49. 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 .

4.50. 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. These are referred to in this chapter as 'non-DII systems' as in many cases these 'systems' are not housed on the DII. In this context the term 'system' is used to mean any aggregation of electronic information which is, or which should be, regarded as a formal record of the MOD.

4.51. Examples include an application database stored on a PC or information generated from a business application such as decision support tool. It may also include information stored in a legacy format on a storage device, for example WordStar™ documents on magnetic tape, or a series of non-DII e-mail messages stored on a PC.

4.52. A challenge for Corporate Memory is to identify non-DII systems which contain information of corporate value and to work with the appropriate business unit to ensure that this information is captured appropriately so that it can be preserved as records. If this hasn't already been done, iHub staff managing information held on non-DII systems (for example operational systems such as Bowman, etc.) must contact the Corporate Memory Records team (see Chapter 2) to discuss the nature of the information held, and potential methods of record capture.

4.53. Corporate Memory has developed a strategic approach, the Non-DII System Record Management appraisal and implementation process, to assess the records management implications of non-DII systems. This is supported by the 'Non-DII System Records Management Appraisal and Implementation Toolkit', which is available on request from the Corporate Memory Records team.

Electronic Records Management in a NTFS (New Technology File System) environment

4.54. Holding records in a NTFS environment must be a temporary measure. Records held in a NTFS environment must be exported into an ERMS as soon as it is available.

Records held in NTFS must be managed in such a way as to support their eventual migration into an ERMS

4.55. Business units with no ERMS capability but with a requirement to maintain their electronic records in an NTFS environment must ensure that business unit work in progress (WiP) documents and records are managed separately.

4.56. The following instructions must be followed when creating an NTFS document and record store:

4.56.1. IHub staff must create two NTFS file plans. One of these will hold WiP documents, the other will contain records.

4.56.2. IHub staff must make users aware that information (WiP and records) should only be stored at the lowest level (folder level) of the file plan.

4.56.3. IHub staff must create a text file called 'ReadMe.txt' for each folder in the records area with appropriate metadata, including: Name/role of folder owner; keywords; retention schedule; a description of intended content.

4.56.4. IHub staff must establish access permissions in the records file plan so that users effectively have 'Contributor' permissions. Users can therefore declare records (from the WiP area, Outlook etc.) and subsequently read them, but cannot deliberately or accidentally modify or delete any records.

4.57. For certain types of record (for example contracts, deeds etc), it is vital to maintain an original paper copy. In these rare cases, iHub staff must ensure that the record is held on a registered file, following the guidance for physical records set out in Chapter 5, and linked to the related electronic folder.

Migrating from NTFS file structure to an ERMS

4.58. Importing record collections from NTFS shared drives 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.

4.59. Electronic files held in a NTFS environment may possess very little file properties (metadata) compared with similar records 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 record is not feasible. Therefore such records 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.

4.60. Only the records area of the NTFS file plan, i.e. the records that have been deemed beforehand as being worthy of preservation, should be transferred to the record management element of the ERMS. At this point, all relevant metadata will be added automatically to each record in turn by the ERMS.

4.61. The remaining documents held in the WiP area of the file plan should be destroyed or migrated to either a similar NTFS area on the new system or a document management system on the new system for example a team site environment.

4.62. Electronic records must not be stored offline (for example on CDs, DVDs), as this makes them difficult for users to discover/access, and risks them becoming inaccessible due to media obsolescence.

Part 3 – Guidance for Project Management Teams introducing an Electronic Records Management System (ERMS)

4.63. The following instructions apply only to project management teams introducing ERMS into business units that will not migrate to DII.

4.64. Project management teams responsible for the selection, configuration and implementation of ERMS in MOD must liaise with the Corporate Memory Records team (see Chapter 2) to ensure that:

4.64.1. The ERMS and associated processes are consistent with Defence-wide policy and processes.

4.64.2. Good industry standards for scalability, maintainability, support, help facilities and documentation are considered.

4.64.3. Appropriate declaration, indexing and retrieval mechanisms exist for electronic records.

4.64.4. The electronic records remain usable for as long as they are required by the business unit. This means that it should be possible to retrieve, use and rely on them.

4.64.5. 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.

4.64.6. Actions carried out can be audited.

The ERMS must facilitate the easy declaration and retrieval of records by users

4.65. Electronic records management must be made as easy as possible, particularly at the record declaration stage, with as few mouse clicks as possible required to effect each transaction.

4.66. Ideally, 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.

4.67. The mechanisms for the capture of records must ensure that:

4.67.1. All types of record are captured[10].

4.67.2. Complete records are captured, for example an e-mail and its associated attachment, are stored together in a meaningful and useful manner.

Records held in the ERMS must be fully searchable

4.68. All MOD records must be readily available to support business and operational needs, and to enable the Department to meet its statutory obligations under Freedom of Information (FOI), Environmental Information Regulations (EIR), etc. Consequently, records must be searchable regardless of whether they are stored online in an ERMS, or elsewhere.

[10] The 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 (for example all hyperlinks may not be stored) and active databases (ERMS may only store regular ‘snapshots’ of information)

4.69. However, the performance of the ERMS should not slow users down. Users should be able to search quickly and efficiently.

4.70. The project team must ensure that the ERMS has a range of in-built search capabilities and the following functionality as a minimum:

4.70.1. The capability to browse and navigate through a file plan structure and allow the selection, retrieval and display of electronic folders and their content through this mechanism.

4.70.2. Full-text content searching.

4.70.3. The capability to create and store saved searches, making them available to all end users.

4.70.4. Advance search capability.

The ERMS must capture appropriate metadata and maintain its links to the records

4.71. 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.

4.72. 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 should be generated by the system or inherited from the upper levels of the business unit file plan, thus saving the user from having to enter large amounts of metadata for a record.

4.73. The e-Government Interoperability Framework (e-GIF) has been mandated for use throughout government. The e-GIF defines the technical policies and specifications governing information flows across government and the public sector. The e-Government Metadata Standard (e-GMS) lays down the framework to be used by government officers when creating metadata for their information resources. The e-GMS is part of e-GIF and forms the basis of the MOD Metadata Standard (MMS) and JSP 717: Using the MOD Metadata Standard, which together establish appropriate metadata capture throughout MOD.

4.74. Compliance with JSP 717 and the MMS is a mandatory requirement on all ERMS implementations.

4.75. The MMS is not intended to be a comprehensive list of metadata items to be used in the MOD as the list of potential metadata elements is almost limitless. Therefore before adopting any optional metadata elements, the project management team must refer to JSP 329: Information Coherence for Defence, to check for potential clashes with MOD controlled terms.

The system must be able to grant and/or restrict access to records in order to meet business, security and legal requirements

4.76. The key characteristics of an effective approach to managing the security of and access to records are described in JSP 440. The project management team must ensure that the ERMS supports:

4.76.1. Confidentiality: access to records is granted only to those who should have it.

4.76.2. 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. The ERMS must ensure that it is not possible for users 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.

4.76.3. Availability: the protection of the record from system downtime, sabotage, malicious damage, theft, fire and flood.

4.77. It is unlikely that the ERMS will be implemented in isolation from other information systems. These systems will make use of existing security services and must comply with existing System Security Policies (SSP). The ERMS implemented will need to operate within that SSP. The project management team should contact their security authority for advice.

The ERMS must contain a series of pre-defined retention schedules

4.78. Users and iHub staff must not be able to create their own retention schedules within the ERMS. IHub staff should be able to select an appropriate retention schedule and apply it to a class/folder as necessary.

4.79. The retention schedules to be used are, review:

- 1 year from date of folder part closure.
- 7 years from date of folder part closure.
- 15 years from date of folder part closure.
- 25 years from date of folder part closure.

4.80. A two month retention schedule is also available. This schedule must only be applied to 'DeleteMe' type classes that have been created to contain folders that have been created in error or for duplicate documents which have been filed by mistake.

4.81. If there is a perceived need to alter/diverge from these retention schedules, project management staff are to contact the Corporate Memory Records team (see Chapter 2) for guidance.

The ERMS and any actions performed within it must be fully auditable

4.82. Audit is required especially for those business units where there is a strong requirement to demonstrate the authenticity of the record.

4.83. 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.

4.84. Audit requires that all operations performed and procedures used to achieve long term preservation of electronic records are clearly defined, and project management staff must ensure that the responsibility for undertaking this definition is appropriately assigned.

4.85. 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. The ERMS should be capable of recording all such actions.

4.86.   Although it is possible for the 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 project management 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.

4.87.   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.

4.88.   Audit trails should be provided for all records. Audit trails should be kept securely, and are made 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.

Electronic records stored in ERMS must be managed in such a way as to demonstrate their evidential weight

4.89.   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".

4.90.   The ERMS should, as far as possible, seek to comply with the provisions of BS 10008:2008 Evidential Weight and Legal Admissibility of Electronic Information (formerly 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 BS 10008 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?

4.91. The compliance workbook for use with BS 10008, BIP 0009:2008 Evidential Weight and Legal Admissibility of Electronic Information, is designed to establish the compliance of a document management system with BS 10008. 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 ERMS and the records within it comply with the recommendations in BS 10008.

Electronic records must be held in a manner such that they will be accessible and usable in the future

4.92. By definition an ERMS should preserve the records held and prevent accidental or deliberate modification or deletion. A digital continuity / 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.

4.93. If records are to be preserved in a usable form, consideration must be given to the metadata required to ensure continued accessibility and to demonstrate their authenticity and integrity. Preservation of documents without their contextual metadata will compromise any digital continuity strategy.

4.94. Project management staff must ensure that electronic records are accessible and usable for as long as they are needed, and that the risks of technological and media obsolescence are addressed. This must be achieved by ensuring that the digital continuity strategy directs project management staff to implement the processes and solutions in accordance with TNA technical standards and guidance on digital continuity.

The ERMS must be able to support the transfer of records between systems

4.95. Once an ERMS has been adopted, it may be necessary to transfer a folder containing records or a series of folders to another ERMS.

4.96. 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. Therefore the ERMS export mechanism must:

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

4.97. 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.

4.98. It is therefore extremely important that the ERMS has a capability to export, and by implication import information to and from other ERMS environments.

4.99. 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.

Chapter 4 – Annex A

File Plan for the Electronic Records Environment

4A.1. The following file plan methodology has been developed and agreed by representatives from all the TLBs and applies to those business units creating a new file plan in an ERMS.

Introduction

4A.2. The introduction of a new file plan methodology, which is based on the functional breakdown of a business unit rather than on how the business unit is organised or structured has been mandated for use across Defence.

4A.3. All business units must put this file plan methodology into practice by April 2012, but implementation should be done at a time that best suits the business unit. This can be when the business unit migrates to DII/F or when the business unit performs an organisation change which provides it with the opportunity to use this methodology.

4A.4. The top level of the Defence file plan is constructed using the following terms:

- Army
- Central
- Estates
- Joint Ops
- Acquisition
- HQ NI
- RN
- RAF
- Science

4A.5. Business unit Information Managers are to ensure that their file plan is implemented in the correct part of this construct so that for example, DE&S business unit personnel are able to file their records under the Acquisition class.

4A.6. The defence file plan methodology begins beneath this top level construct.

File Plan Methodology

4A.7. The file plan will comprise of 4 sections or classes and start at the first level below an approved Electronic Unit Name (EUN). These **Level 1** classes are:

01 **Administer** *the Unit*
02 **Command** or **Direct** or **Manage** *the Unit*[11]
03 **Support** *the delivery of the Unit's objectives*
04 **Deliver** *the Unit's objectives*

4A.8. With the exception of the Deliver class, this methodology prescribes a number of optional **Level 2** classes. Business units must develop their file plan by choosing only from these level 2 classes. The level 2 classes comprise of the following:

[11] The TLB SIO must decide which one of the three terms the organisation will use.

LEVEL 1	**LEVEL 2**	
01	**Administer** the Unit	
	01_01	Manage Accommodation
	01_02	Manage Compliance
	01_03	Manage Estate
	01_04	Manage Military / Branch Matters
	01_05	Manage Personnel
	01_06	Manage Relations
	01_07	Manage Resources
	01_08	Personal Development
	01_09	Provide Office Services
	01_10	Provide Travel Services
	01_11	Provide Welfare Services
02	**Command** or **Direct** or **Manage** the Unit	
	02_01	Conduct Planning
	02_02	Issue Orders and Instructions
	02_03	Learning From Experience
	02_04	Manage Executive
03	**Support** the delivery of the Unit's objectives	
	03_01	Conduct Information Management
	03_02	Manage Communication Services
	03_03	Manage Projects
	03_04	Provide Commercial Activities
	03_05	Provide Equipment / Engineering Services
	03_06	Provide Fire Services
	03_07	Provide Health Services
	03_08	Provide Installation Security
	03_09	Provide Intelligence Activities
	03_10	Provide Logistics Support
	03_11	Provide Training Activities
	03_12	Support *Activity*[12] Operations
04	**Deliver** the Unit's objectives	

4A.9. The level 2 classes created by business units under the 'Deliver the Unit's objectives' class can best be described as a functional analysis of the business unit's activity. These classes should ideally reflect a breakdown of the business unit's business or management plan and the activities the business unit conducts to deliver against this plan.

4A.10. Full descriptions for each **Level 1** and **Level 2** class can be found in Appendix 1.

4A.11. Beneath the level 2 classes, will be a number of subordinate classes and ultimately the folder. This construct makes up the business unit file plan. The file plan must be no more than 6 levels deep with the folder making up the 6th level.

4A.12. How the file plan is implemented within an organisation is for the TLB SIO to decide. The SIO can choose to adopt a centralised or distributed form of the file plan to suit the needs of the organisation. However the single class at the top of the business unit file plan must represent an approved EUN.

[12] This Class is a top level class for those organisations who have a number of activities relating to the delivery of specific, peculiar to role activities such as Air Traffic Control, which are required by some units but are not standard across defence.

Centralised Approach

4A.13. By adopting a centralised approach, the file plan can be implemented at TLB level (the very highest level of the business unit organisation). In this case the TLB SIO will direct that all its subordinate business unit personnel use this file plan to store their records. The file plan will be managed by the TLB Information Manager (IMgr). This approach is perhaps more suitable for smaller business units. This is shown below in Diagram 1.

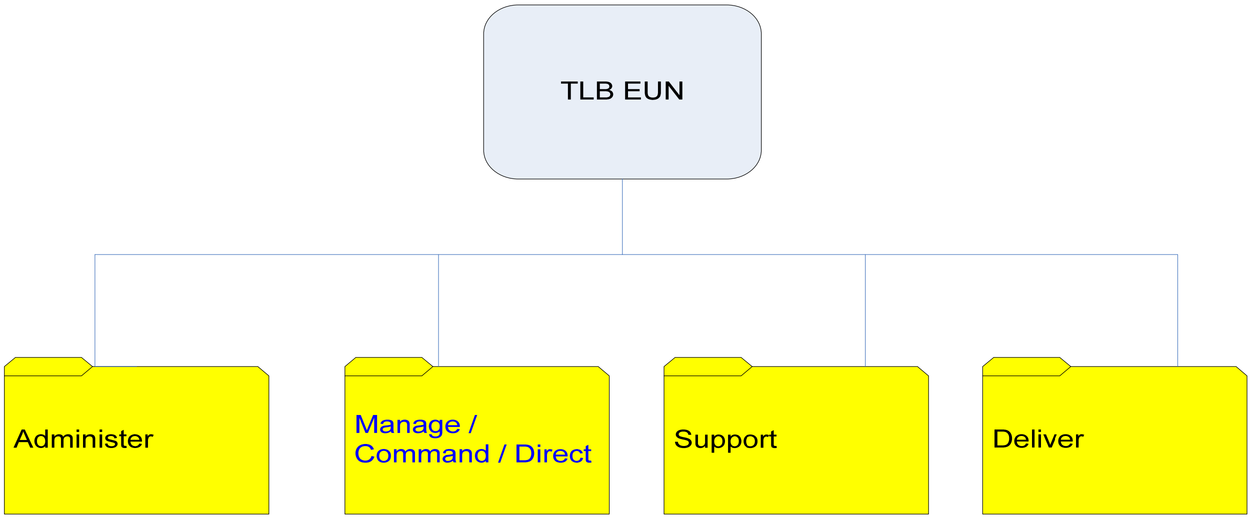


Diagram 1 – Centralised File Plan

Distributed Approach

4A.14. The TLB SIO can choose to implement a distributed file plan for the TLB where this methodology would be implemented at subordinate (HLB or below) levels of the organisation. This approach is perhaps more suitable for larger TLB organisations as it allows each subordinate business unit IMgr to manage their own part of the file plan. Also business unit personnel are able to drill down to a more recognisable area of the file plan where they can file their records. This approach is illustrated in diagram 2.

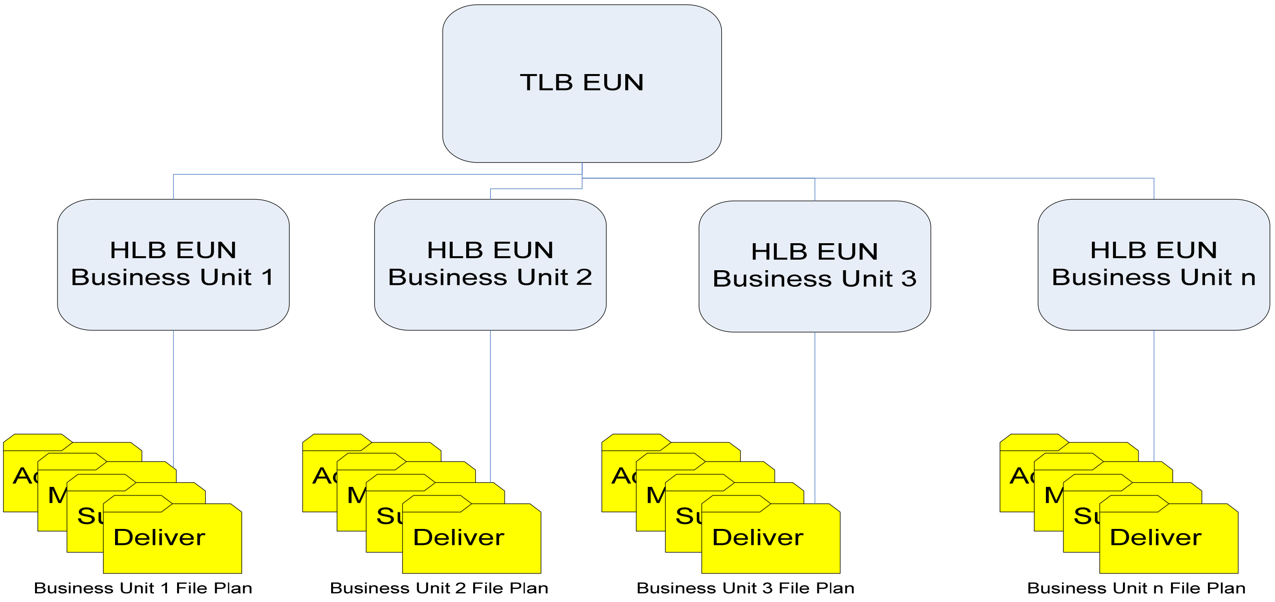


Diagram 2 – Distributed File Plan

4A.15. Regardless of how business units implement the file plan the following rules are to be complied with.

File Plan Rules

4A.16. The Level 1 classes are mandatory and they are to be present in all MOD file plans. It is expected that all four Level 1 classes will be populated with further classes. Business units must use the Level 1 class names as prescribed above or in Appendix 1.

4A.17. It is expected that a number of the optional Level 2 classes will be selected. If selected, business units are to use the Level 2 class names as prescribed above or in Appendix 1.

4A.18. The subordinate classes below ‘Deliver’ are to be determined by the business unit IMgr and must reflect a functional breakdown of business unit activity.

4A.19. The file plan must be no more than 6 levels deep, where level 6 is a folder. Remember:

4.19.1. A class can contain other classes or folders but not both, and never records.

4.19.2. A folder consists of folder parts that may only contain records or physical markers (no sub-folders) and is always at the lowest level of the file plan.

4A.20. Levels 2 to Level 6 of the file plan are to be defined by the business unit IMgr.

4A.21. Only iHub personnel are to have the permissions to modify the file plan.

4A.22. A minimum of one taxonomy term is to be applied to each Level 2 class used in the file plan. These terms can be found in Appendix 1 and are used to assist iHub personnel when applying taxonomy terms to subordinate classes and folders.

4A.23. A minimum of one taxonomy term is to be applied to each subordinate class and folder.

4A.24. One retention schedule is to be applied to each Level 2 class used in the file plan. A list of generic retention schedules can be found in Appendix 1 and are to be used to assist iHub personnel, under the direction of the Information Manager, when applying retention schedules to folders.

4A.25. One retention schedule is to be applied to each subordinate class and folder.

4A.26. According to the nature of the records and information to be stored within, reduced (or limited) permissions are to be applied at the lowest possible level of the file plan and in most cases these limitations must be applied at folder level.

4A.27. Meaningful descriptions must be used to identify subordinate classes and folders. Terms such as "General", "Miscellaneous" and "Policy" are too vague to be appropriate for use as class and folder names and must be avoided. All subordinate class and folder names should be specific and clearly identify the nature of the material to be contained within the folder.

4A.28. The following special characters must not be used when labelling class or folder names: \ / ‘ ! ( ) , : ; @ * ? “ ” < > + £ = ¦ { } [ ] ^ % & ~ #.

4A.29. Acronyms and abbreviations should only be used where they are well known and unambiguous, for example FOI is well understood whereas TNA could be either The National Archives or Training Needs Analysis.

4A.30. Any class or folder of the file plan to which access has been limited is to be represented by the inclusion of the capital letters LTD at the end of its name.

4A.31. Where business units operate in both SECRET and RESTRICTED domains, then a file plan must exist for both domains. However there is no requirement for the SECRET file plan to be a replica of the file plan in the RESTRICTED domain.

4A.32. Any class or folder of the file plan which exist in both the RESTRICTED and SECRET domains must be represented by the inclusion of capital letters R-S at the end of the folder name.

4A.33. Duplication of subordinate class and folder names must be avoided.

4A.34. The use of a file numbering system is not mandatory. However, if business units use file numbers[13] they must be used throughout the file plan, and:

- The file number must be preceded by an approved EUN.
- The file number must reflect the numbering format shown in the table above and in Appendix 1. For example, if you pick two classes from Level 2, ‘01_01 Manage Accommodation’ and ‘01_03 Manage Estate’ you cannot renumber Manage Estate to ‘01_02’ just to keep the sequence.
- Each element of the file number should be separated by an appropriate character to distinguish each individual class and folder. The following special characters are not to be used as separators: \ / ‘ ! ( ) , : ; @ * ? “ ” < > + £ = ¦ { } [ ] ^ % & ~ #.

[13] An example of a file number to reflect a folder under Manage Compliance is TLB EUN_01_02_03_04. Where the folder relates to a potential activity under Audit [03], for example Audit Procedures [04].

Annex A – Appendix 1

File Plan Class Descriptions with Taxonomy Terms and Generic Retention Schedules

Serial	Level 1 Class Name		Description	Potential Activities	Taxonomy Classification	Generic Retention Schedule (Review X years after date of last entry unless otherwise specified)
		Level 2 Class Name				
01	***Administer*** the ***Unit***		The range of activities that enable the business unit's management to support its physical infrastructure and human resources.		N/A	N/A
	01_01	Manage Accommodation	The allocation and management of existing accommodation (domestic, office, technical or mess deck accommodation and compartments whilst onboard ship) and the provision of services for the daily maintenance and support of people using that accommodation. This will also include using shore-side facilities whilst ships are in build or refit and the provision of facilities management services for the daily maintenance and support of those facilities.	• Catering Services • Removals • Mess Committee Activities • Officers' Accommodation • Senior Rates Accommodation • Junior Rates Accommodation • Shared facilities for lodger units • Communal Messes • Office Accommodation • Technical Compartments • Facilities Management	• Built Estate • Overseas Estate	7 Years

	01_02	Manage Compliance	The range of activities involved in the management of all common activities required for the protection of the business unit and its staff from legal challenge or litigation. This section will include the sub-class 'Maintain Historical Record' for Army Units.	• Governance • Audit • Scrutiny • Assurance • Legal – FOI / DPA • Equality and Diversity • Parliamentary – Questions / Debates • Ministerial – Enquires / Submissions • Quality Management • Quality Assurance • Security – Vetting / Personnel / Physical / IT • SHEF - Health and Safety • Environmental Protection – Fire / Nuclear • Disaster Recovery • Gifts and Hospitality • Inspections • Flight Safety • Historical Record • Monthly Unit Report	• Safety • Parliamentary and Ministerial Business • Security and Intelligence • UK Legislation • Claims and Compensation • EU Legislation and Agreements • International Law and Agreements • Sustainable Development and Environment	25 Years
	01_03	Manage Estate	The provision of building and other capital infrastructure projects in developing the business unit accommodation. Includes the provision of facilities management services for the daily maintenance and support of the building.	• Accommodation Stores Contracts • Facilities Mgt – Contracts / Services • Work Services Contracts • Buildings • Estate Management • Property Management • Utilities	• Estate Strategy and Management • Estate Maintenance Services	25 Years
	01_04	Manage Military / Branch Matters	Activities involved in the management of specific military issues relating to the business unit or to attached personnel.	• Museum Information • Dress Information • Association Information • Individual Branch Matters	• Ceremonial and Drill Operations • Service Personnel	25 Years

	01_05	Manage Personnel	All personnel and human resource management activities in support of the business unit, including all manpower issues, discipline, pay, casualty, awards, selection, duties and industrial relations. The contents of this class are likely to be subject to access restrictions and may require casework files.	• Discipline • Recruitment • Selection • Manpower • Industrial relations • • Pay Personnel • Personnel Administration • Personnel Issues • Personnel Security (including Vetting Activity) • Honours and Awards • Allowances • Casualties • Establishment • Watch and Quarter Bill • Duty Personnel	• Personnel • Allowances (non-pay) • Allowances (pay-related and permanent) • Allowances policy • Career development and management • Charitable activities • Conduct • Discipline • Employee relations • Employment terms and conditions • Equality and diversity • Grading ranks and job evaluation • Honours and awards • Leaving the MOD and the Services • Manpower policy and planning • • Pay Pensions and compensation schemes • Performance • Personnel administration and management • Personnel strategies and plans • Recruitment and retention • Reserve service • Skills and competences frameworks • Sports hobbies and social activities • Veterans • Working hours and leave	25 Years (But with the intention of retaining some categories for 100 years.)

	01_06	Manage Relations	The maintenance and projection of the business unit's image to external stakeholders including other MoD organisations and the public. Relevant information includes visits documentation and public relations information.	• Communications • External events • Internal Events • Meetings • Port Visits • Visits • Public relations Management Information • Performance Management • Civil Military Co-operation (CIMIC) tasks that are not included as part of the business unit's core output. • Units Liaisons • Units Affiliations • Units Charities • Trade Unions	• Corporate Communications and Image • Internal Communications • Public relations • Defence In the Wider Community • Military Aid to the Civil Authority • Peace Support Operations	7 Years 25 Years - Policy Records
	01_07	Manage Resources	Central management of all the business unit's resources (excluding manpower) including budgets and finance, hospitality and resource accounting.	• DRAC • Budget Management • Budgets and Finance • Fixed Assets • Finance / IYM • Stock Accounting • Letters of Delegation • Balanced Scorecard • Organisation Structures • Resource Accounting • Public and Non Public Funds • Hospitality • Official Entertainment	• Financial Management • Defence Budget Life Cycle	7 Years

	01_08	Personal Development	The common development of the business unit's personnel or human resources through formally and informally delivered training activities. Includes physical education, common core skills instruction and all mandatory training (for example Military Annual Training Tests). Includes organised sport and adventurous training, maintenance of Operational Performance Statement (OPS), personal educational development, Command, Leadership and Management (CLM) training and resettlement. Does not include training that forms part of a business unit's core objectives.	• Personal Training • Induction Training • Adventurous Training • CLM Training • Organised Sport • Achievement of OPS • Resettlement Courses • Physical Education • ECDL • Qualifications • Reporting	• Personnel • Allowances (non-pay) • Allowances (pay-related and permanent) • Allowances policy • Career development and management • Charitable activities • Conduct • Discipline • Employee relations • Employment terms and conditions • Equality and diversity • Grading ranks and job evaluation • Honours and awards • Leaving the MOD and the Services • Manpower policy and planning • Pay • Pensions and compensation schemes • Performance • Personnel administration and management • Personnel strategies and plans • Recruitment and retention • Reserve service • Skills and competences frameworks • Sports hobbies and social activities • Veterans • Working hours and leave	25 Years

	01_09	Provide Office Services	General administrative management of the work place, including stationery and office machinery.	• Accommodation Stores • Office Equipment • Postal Service • Stationery	• Accommodation Stores and Office Equipment	1 Year
	01_10	Provide Travel Services	The provision and management of air, road and rail travel for business units served by locally run travel offices. Provision of transport related services in support of the business unit, including travel and movements. Movement services directly related to an Operation, Exercise or task will be held with all other information related to that activity.	• Hotel Accommodation • Transport	• Travel and Transport Services • Air movements management • Sea movements management • VIP transport	7 Years
	01_11	Provide Welfare Services	Support of and providing for the well being of the personnel in the business unit. Includes community work such as that done by the business unit personnel, social teams, chaplaincy and any charitable work.	• Welfare • Community Work • Social club activities • Chaplaincy • Charity work	• Personnel • Veterans • Welfare and Family Support • Welfare and Charitable Organisations	7 Years

02	***Command / Direct / Manage /*** the ***Unit***		The range of activities that direct the business unit’s long-term plans or strategy, set and report on management objectives and undertake decision making at the executive level.		N/A	N/A
	02_01	Conduct Planning	The creation of a management plan and reporting against those objectives. The receipt of and response to tasking and the creation and maintenance of contingency plans. The contents of this class are likely to be subject to access restrictions.	• Strategic Policy • Business Unit Plans • Benefits • Contingency Planning	• Performance Management • Command and Battlespace Management	15 Years
	02_02	Issue Orders and Instructions	The creation, issue, publishing, maintenance and update of business unit orders, instructions, generic policy and procedures. Specific policy and procedures such as Safety, Health, Environment and Fire (SHEF) Policy and security orders would be held under the relevant section.	• Policy • Strategy • Standards • Internal Inspections/Audit • Standing Orders • Daily Orders • Standing General Orders (SGOs)	• Defence Policy & Strategic Planning • Counter-proliferation and arms control • Counter-terrorism policy • Defence diplomacy • Defence in the wider community • European Union defence policy • Home capability policy • International relations • International security and defence • Operational capability • Strategic policy making • Trade relations	15 Years

	02_03	Learning From Experience	The lessons identified and learnt as a result of experiences gained from a conflict, operation, exercise or project. Specific policy and information relating to the conflict, exercise or project would be held under the relevant section.	• Lessons Identified • Lessons Learnt	• Learning from experience	25 Years
	02_04	Manage Executive	Managing the efficient working of the business unit’s command / executive decision making roles and bodies. The contents of this class are likely to be subject to access restrictions.	• Inputs to and outputs from Command meeting • Communication from the executive (both internally and externally) • The conduct of any Command visits or management programme. • Commanding Officers personal correspondence that CANNOT be placed within a functional area.	• Corporate Leadership	15 Years

03	***Support*** the delivery of ***Unit*** Objectives		The range of activities conducted in the direct support of delivering the business unit's objectives. The mix of activities is highly dependent upon the nature of the business unit and must be closely mapped to the contents of 'Deliver Unit objectives'.		N/A	N/A
	03_01	Conduct Information Management	Supporting and enabling the correct management of the business unit's information assets and promoting the exploitation of those assets. Includes the functions of the iHub and any common or cross-organisation information analysis.	• Business Management • Business Continuity • Business Operations • Business Case Mgt • Information Exploitation • Information Administration	• Information Management	5 Years
	03_02	Manage Communication Services	The provision of communications services for the business unit or the management of service provision for outsourced communications services. Will include domestic radio, telephony and information systems such as DII. Management of specific software applications in support of functional areas should be included within the relevant functional sections.	• Domestic radio • DII • Standalone equipment and software • Telephony	• Communication Services	Length of contract + 7 Years
	03_03	Manage Projects	The management of the delivery of change within the business unit. The contents of this class are bounded by the scope of each change project and will change as projects begin and are closed.	• Change Management	• Project Management • Programme Management	Length of project + 7 Years
	03_04	Provide Commercial Activities	Provision of commercial services which are normally delivered by outsourced agencies.	• Low Value Purchasing • Contracts • Enterprise Agreements	• Procurement process • Contract management • Commercial management	Contract length + 7 years

	03_05	Provide Equipment / Engineering Services	Provision of equipment support at 1st line. Dependent upon the nature of the business unit, such support may have been outsourced either to a civilian contractor or a MOD depth organisation.	• Local Air Defence activities • Provision of engineering functions	• Support Chain • Operational Logistics Support	15 Years
	03_06	Provide Fire Services	Provision of emergency fire services to the business unit. These functions are usually delivered by Defence and, dependent upon the nature of the business unit, may be treated as outsourced services.	• Includes the provision fire cover for airfield crash plans.	• Fire Service Operations	15 Years
	03_07	Provide Health Services	Delivery of health services, including dental services, to business unit personnel. These functions are usually delivered by Defence and dependent upon the nature of the business unit, may be treated as outsourced services. Health services directly related to an Operation or Exercise will be held in the relevant folder under the Operation or Exercise class. This will ensure that all health records pertaining to the Operation or Exercise are held together. The contents of this class will be subject to access permissions.	• Includes the provision of medical cover for airfield crash plans. • Medical • Dental	• Primary Healthcare • Secondary Healthcare	25 Years

	03_08	Provide Installation Security	Provision for all aspects of the business unit’s security. The contents of this class are likely to be subject to access restrictions.	• Maritime Security • Personnel Security (excluding Vetting Activity) • Physical Security • Documentary Security • Information Assurance • Force Protection	• Access control systems and equipment • Communications security • Cryptography and key management • Defence policing • Industrial security • Information security • Information technology security • Nuclear security • Operations security • Personnel security • Physical security • Scientific and technical security • Security policy and management	15 Years
	03_09	Provide Intelligence Activities	The range of activities involved in the dissemination of generic Intelligence information in support of the business unit. The contents of this class are likely to be subject to access restrictions.	• Direct Intelligence • Collect Intelligence • Process intelligence • Disseminate Intelligence • Operational briefing Material • Threat assessments	• Communications security • Counter-terrorism • Intelligence cycle • Security policy and management • Threats crimes and civil emergencies	25 Years

	03_10	Provide Logistics Support	Provision of logistics support to the business unit. Includes both forward and depth elements of logistics support, including logistics personnel, catering services, hotel services and the materiel supply chain. Dependent upon the nature of the business unit, parts of such services may have been outsourced either to a civilian contractor or a MoD depth organisation. Logistics Support information directly related to an operation, exercise or task will be held with all other information related to that activity.	• Logistics Personnel • Catering Services • Hotel Services • Supply Chain	• Operational Logistics • Support Chain • Supply Chain	15 Years
	03_11	Provide Training Activities	The provision of all aspects of internal operational training exercises. For Royal Navy, will Include CBRN, First Aid training etc. in order to protect the business unit from all threats including a CBRN environment or war fighting situation. Does not include Adventurous Training exercises.	• Training Needs Analysis	• Defence Training Estate • International Defence training and education • Operations and operational training • Training and education	7 Years

	03_12	Support ***Activity*** *Operations*	The direct management and coordination of operational effort across the business unit in the delivery of operations support services. This class would normally only be used where an organisation uses a static location as the base for operations, i.e. an airfield or port. An organisation may have any number of such sub-classes, each relating to a specific output activity (for example, Air Traffic, Port Ops, Rail Ops). These sub-classes would sit below this class in the file plan.	• Operation [by Name] • Operational Planning • Provide Air Dept Services • Provide Executive Services • Provide Warfare Support • Support Assault Squadron RM • Support Embarked Staff	To be determined by the IMgr.	To be determined by the IMgr.

04	***Deliver*** the ***Unit*** Objectives		The range of activities which deliver the outputs of the business unit. These activities are specific to each business unit; however, where a number of business units exist with similar purposes (such as training) the contents of this class should be similar in each such organisation. Sub-classes are to be derived which reflect the outputs or objectives of the business unit based upon the contents of its management plan.		N/A	N/A
	04_01-n	***Tasks or objectives as required***	The range of activities and outputs that directly relate to a task or output. It will include the full range of output activity including cross output activities such as training and meetings/conferences specific to the task. A business unit may have many of these classes. For formed units deploying on operations under the OPCOM of CJO, this section of the unit's file plan will be mandated by PJHQ.		To be determined by the IMgr.	To be determined by the IMgr.

CHAPTER 5

The MOD Filing System – Paper Records

The File Plan

5.1. The guidance for the creation and maintenance of a business unit file plan for paper files is described in Chapter 5 Annex A and is particularly useful for units involved in reorganisations or mergers.

Registered Files

5.2. MOD, in common with other government departments, operates a paper filing system to account for the use of registered files where each file relates to a particular subject, or aspect of a subject identified in the file plan.

Contents of a Registered File

5.3. 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 are to be destroyed when no longer needed.

5.4. Purpose-designed registered file covers (listed below) must be used and are to be ordered from Forms and Publications Commodity Management, using MOD Form 999. Details of the ordering process can be found in DIN 2008DIN04-049. See also Chapter 5 Annex C.

- **TOP SECRET** (Red) - MOD Form 329A;
- **SECRET** (Pink) - MOD Form 329B;
- **CONFIDENTIAL** (Green) - MOD Form 329C;
- **RESTRICTED/Unclassified** (Buff) - MOD Form 329D.

5.5. 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.

Opening a Registered File

5.6. When creating the registered file the following actions must be carried out:

- The full file title, as it appears in the file plan, 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 must 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 Registered File Record Sheet (MOD Form 262A)

5.7. 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 must be recorded on the MOD Form 262A in the designated area.

5.8. The MOD Form 262A 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 (preferably MOD Form 262, but A4 lever-arch binders are acceptable) and maintained until replaced by a Registered File Disposal Form (MOD Form 262F).

5.9. If a registered file is sent temporarily to another business unit the MOD Form 262A 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.

5.10. The MOD Form 262A 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.

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

Placing Documents onto Registered Files

5.12. You must 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.

5.13. 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, for example E1, E2, etc.

5.14. Late enclosures should also be filed in date of origin order. This will mean inserting them between existing closures. Existing enclosure numbers must 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; for example 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, for example in this case E2+3.

5.15. 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.

5.16. The protective marking of the registered file cover is to correspond to the highest protective marking of its contents. For example, a file may contain a majority of not protectively marked information and only one TOP SECRET document. This file will be classed as TOP SECRET. Should a RESTRICTED/unclassified file exist and a new document protectively marked as “CONFIDENTIAL” or above need to be placed on it, the file is to be upgraded.

The File Minute Sheet

5.17. The file minute sheet is a plain piece of A4 paper that is held on the left-hand side of the file. Each minute should be numbered and the protective marking of the minute should be indicated. The file minute sheet 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 the DBS KI Records Review team.

5.18. When a file is being passed to a colleague for action, the covering minute can be used to record the exchange and any decisions reached. When referring to colleagues, the boxes on the front of the file must be used. Remember to include the minute or enclosure number, the title of the person to whom the file is being referred and the date when referred.

Transfer of Enclosures between Registered Files

5.19. When an enclosure has been misfiled and the action is to remove the item, the following information should be recorded on a sheet of plain 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.

5.20. 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.

Temporary Enclosure Jackets

5.21. 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[14] of appropriate protective marking and forwarded to the appropriate business unit, bearing the following information:

- A separate MOD Form 262A must be raised to record the existence of the TEJ and to whom it has been sent.
- The TEJ must 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 must bear the file reference and title of the parent file with the addition of its own TEJ number, for example "TEJ NO 1" and so on.

5.22. The TEJ must be returned to the originating business unit and the enclosures incorporated into the parent file as soon as possible and any surplus photocopies destroyed. There may be occasions when the TEJ will need to be incorporated into the parent file in its entirety for example when the non-availability of the parent file has meant that a significant number of papers together with a record of key decisions have been the result. When this has happened the TEJ must be incorporated into the file through the following means:

- It must be placed in the file in date order (according to the date returned which should be marked on the TEJ cover).
- It must be allocated an enclosure number.
- The file minute sheet must be annotated to record the enclosure number of the TEJ along with details of the number of enclosures contained within it.
- The MOD Form 262A associated with the TEJ must 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.

5.23. Purpose-designed TEJs should be used and can be ordered from Forms & Pubs Commodity Management. See Chapter 5 Annex C for more details.

Record of Protectively Marked (SECRET and TOP SECRET) Documents

5.24. In addition to the previously described requirements of a registered file there are extra requirements for registered files protectively marked as "SECRET" and "TOP SECRET".

[14] MOD Form 174A (TOP SECRET),
MOD Form 174B (SECRET),
MOD Form 174C (CONFIDENTIAL) and
MOD Form 174D (RESTRICTED/Unclassified)

5.25. Along with the file minute sheet, a "Record of Classified Documents (TOP SECRET and SECRET)" (MOD Form 672) form must be placed on the left hand side of the file.

5.26. When an enclosure protectively marked as SECRET or TOP SECRET is placed on a file, its existence and enclosure number must be recorded on MOD Form 672 and also entered into the Protected Document Register (MOD Form 102).

5.27. The instruction for maintaining, sending and receiving protectively marked material is contained within JSP 440: The Defence Manual of Security, Part 5 Section's 2 and 3. This guidance also includes retention periods for the MOD Form 102 and the storage requirements for such material.

Upgrading Registered Files

5.28. It will sometimes be necessary to upgrade a file to reflect the fact that a new enclosure is of a higher protective marking than the existing file. When this is the case, a new file cover must be produced and given an identical number to the old cover.

5.29. The contents of the old file must 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.

5.30. The date of opening of the original file must be entered on the front cover of the upgraded file (for example not the date on which the file was upgraded). The date on which the file was upgraded must be entered beneath the date of opening. The MOD Form 262A must also be amended to show the date of upgrading, along with the new protective marking.

5.31. 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.

5.32. MOD Form 672 must be placed in the file (for SECRET and above).

5.33. The document that triggered the upgrade of the file must be recorded in the MOD Form 102. Details on the completion and management of MOD Form 102 can be found in JSP 440 Part 5, Section 2, Chapter 2.

5.34. File covers denoting a protective marking higher than the first enclosure(s) are not to be used in anticipation of material which might be placed on the file later.

Access to Registered Files

5.35. All MOD personnel are required to share information responsibly and sensibly. Sensitive records about individuals and records that are protectively marked must be labelled accordingly and access limited to those who genuinely need them to perform their duty. If you do not handle information in compliance with JSP 440: The Defence Manual of Security and the Data Protection Act, you may be subject to disciplinary proceedings.

5.36. All MOD personnel should also be aware of their responsibilities as laid down in the Official Secrets Act. In short, it is an offence for anyone to disclose official information where it would be reasonable to expect it to be protected by the Act. See JSP 440 Part 9, Chapter 2, for more details.

5.37. Registered files may be circulated to other government departments or external legal advisers and to the National Audit Office, where appropriate. Registered files must not to be sent to any location apart from the ones mentioned above without the prior approval of Corporate Memory Records DepHd.

5.38. 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]".

Transfer of Registered Files to another Government Department or MOD Business Unit

5.39. If the need arises to transfer a file permanently to another government department, Corporate Memory Records DepHd must be consulted before any transfer action is taken.

5.40. The need may arise to transfer a file or a series of files to another MOD business unit. An example might be when a reorganisation results in the transfer of responsibility for a particular project to a different business unit.

5.41. 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. Corporate Memory Records DepHd should be advised in writing if such action is taken.

5.42. It may however not be practical to retain the existing file number (for example 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.

5.43. 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).

5.44. 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.

5.45. In all cases, the appropriate MOD Form 262A must accompany the transferred files to the "importing" business unit where they should be attached to the new MOD Form 262A. The "exporting" business unit must formally record the transfer of the files in the file plan and may, additionally, retain a copy of the relevant MOD Form 262A annotated to record the transfer. The "exporting" business unit must also notify Corporate Memory Records DepHd of the transfer.

5.46. Where the exporting business unit retains previous (closed) parts of the file they should also be forwarded to the importing business unit. Additionally, any MOD Form 262F held for previous parts of the file should be forwarded.

Missing Files

5.47. If, after a thorough search, a registered file cannot be located, a written report **MUST** be submitted to Corporate Memory Records DepHd. The report is to: identify the file concerned, its protective marking and the nature of its contents; and contain an explanation of the circumstances surrounding its loss. If the file contained protectively marked information a report is also to be submitted to the appropriate security directorate in accordance with the instructions in JSP 440.

Closing a Registered File

5.48. There are a number of factors which need to be assessed when determining whether to close a registered file. If any of the following criteria apply the file **MUST** 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.

5.49. 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 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 must then be completed. This records the retention schedule recommendation.
- 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 Corporate Memory, a B/F (bring forward) date must 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.

5.50. Guidance for completing MOD Form 262F can be found at Annex D to this Chapter.

Reviewing a Closed Registered File

5.51. The following actions are to be taken prior to and during the review of a registered file:

- Insert the MOD Form 262F, completed as above, onto the right hand side of the file (that is to say on top of the last enclosure).
- 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.
- Pass the file to the “owner” or Reviewing Officer to review and complete sections 2 and 3 of the MOD Form 262F.

5.52. On receipt of the file, the Reviewing Officer must:

- Consult Part 1 of MOD Form 262F to determine whether a retention schedule recommendation has been recorded.
- Take account of the retention schedule recommendation and complete Part 2 of the form identifying:
    - ♦ The appropriate retention period for the file.
    - ♦ Any key enclosures that support the recommendation.
    - ♦ Whether at the end of any retention period specified for administrative use, the file merits consideration for permanent preservation.
- Complete and sign Part 3 of the form and return it to the iHub.

"Weeding" of Registered Files

5.53. The weeding of registered files is prohibited. One of the reasons for this is that the process of weeding files is a time-consuming and therefore costly activity. A second reason is that to ensure that preserved documents retain their original context, The National Archives (TNA) requires MOD to select complete files for permanent preservation rather than extracts from files.

Actions to be taken following the Review of a Registered File

5.54. Following the return of the registered file and completed MOD Form 262F, Information Management staff should:

- Note the decision made by the Reviewing Officer;
- Record the relevant B/F action for the file and place 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.)

5.55. When a file is destroyed by the business unit, the MOD Form 262F must be removed and used to replace the MOD Form 262A which must then be destroyed.

5.56. If the file is not destroyed locally but is forwarded to the appropriate 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 MOD Archives and use it to replace the MOD Form 262A, which should then be destroyed.

5.57. MOD Form 262A and MOD Form 262F are the definitive record of a file's existence and subsequent destruction or passage to the MOD Archives. MOD Form 262A must not be destroyed until replaced by MOD Form 262F.

5.58. Each MOD Form 262F must be retained for a period of at least 30 years from the date it replaces the MOD Form 262A.

5.59. As MOD Form 262F are normally retained in a binder (MOD Form 262 or A4 Lever-Arch Binder) relating to a file series or a number of file series, the binders should be retained for a period of at least 30 years following the insertion of the final MOD Form 262F.

5.60. If a business unit is disbanded during this period the forms must be passed to the successor business unit. If there is no successor or parent business unit the binders must be forwarded to the appropriate MOD Archives for storage.

5.61. When files are to be forwarded to the appropriate MOD Archives, care should be taken when completing Section 2 of the form. The file's disposal recommendation should be sufficiently detailed and identify clearly why the file is being recommended for further retention.

5.62. Chapter 5 Annex D provides a practical example of how to complete MOD Form 262F correctly.

Material NOT placed on Registered Files (Unregistered Records)

5.63. 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.

5.64. A ‘Record of Unregistered Material’ must be established describing as a minimum: the nature and format, current location, and date of creation or receipt of all unregistered records held by the business unit.

CHAPTER 5 – Annex A

File Plan for a Paper Based Filing System[15]

5A.1. The guidance which follows relates to the creation of a new file plan for a paper based filing system and is particularly useful for units involved in reorganisations or mergers. The underlying principles should also be applied when file plans are being amended or updated.

5A.2. The file plan follows a hierarchical structure and 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.

The File Plan - Main Headings

5A.3. In creating a hierarchical file plan, the first task is to identify the main headings which will be required. It is impossible to be prescriptive about what these should be 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 list is "Administration"; the other main headings should then be listed in order of significance and be dependant on the Organisation or Establishments key business.

The File Plan - Secondary (or Subsidiary) Headings

5A.4. 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; for example after selecting the main heading of “Administration”, the secondary headings might be subjects like Personnel, Security, Organisation and Training.

The File Plan - Tertiary Headings

5A.5. Having identified the main and secondary headings the same approach is now used to create the tertiary headings: for example “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 plan, a logical and straightforward file index will be created which is consistent and easy to follow.

General Principles of File Headings

5A.6. File titles, which must have a minimum of two headings, should not normally exceed three headings for example main, secondary, and tertiary; where absolutely necessary the use of additional sub-headings is permissible.

5A.7. 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

[15] The guidance for the creation of a new file plan in an electronic records management system can be found in Chapter 4. If a business unit has implemented an electronic or hybrid filing system then the file plan methodology described in Chapter 4 is to be employed.

tertiary headings wherever possible. All headings should be specific and clearly identify the nature of the material to be contained within the file.

5A.8. 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.

File References

5A.9. Each file **MUST** be allocated a unique file reference. This will be an alpha/numeric combination which serves to ensure that a newly created file is not confused with any other file. Each element of the reference should be separated by an oblique stroke (/) to distinguish each individual component.

5A.10. 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.

5A.11. The business unit short 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‘ for example 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 Corporate Memory file plan would appear as:

File Reference Number	Main Heading	Secondary Heading	Tertiary Heading
CIO-CMemR/1/1/1	Administration -	Manage Accommodation -	Removals
CIO-CMemR/1/1/2	Administration -	Manage Accommodation -	Shared facilities
CIO-CMemR/1/1/3	Administration -	Manage Accommodation -	Catering services
CIO-CMemR/2/1/1	Manage -	Planning -	Strategic Policy

5A.12. In the event of a gap in the numbering, the unused number should appear on the file plan but carry the annotation "RESERVED".

Approval of the File Plan and Reference Numbers

5A.13. All organisation and deployed HQ file plans incorporating retention schedules (see Annex B) and associated reference numbers, are to be approved by the Corporate Memory Records team prior to first use.

5A.14. Any proposed changes to main headings or numbers are to be submitted to the Corporate Memory Records team for approval prior to incorporation into the file plan.

5A.15. An up to date copy of the file plan is to be forwarded annually to the Corporate Memory Records team.

General Principles of Creating or Updating a File Plan

5A.16. When creating a new or updating an existing file plan, be aware that if the Directorate or business unit short title is unchanged from the previous file plan, 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.

Maintenance of an Approved File Plan

5A.17. The Information Manager must maintain a definitive copy of the file plan which should be amended when new files are created; changes are made to the disposal recommendation or change of “owner” of the file. The Information Manager has ultimate responsibility for the maintenance of the file plan though day-to-day responsibility may be delegated to the iHub or administrative supervisor.

5A.18. The completed file plan must incorporate a retention 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 retention schedule is contained in Chapter 7.

CHAPTER 5 - Annex B

Example of a Completed Retention Schedule

Ref No.	Main Heading	Secondary Heading	Tertiary Heading	Retention Schedule Recommendation	Explanation of recommendation
1/1/1 1/1/2 1/1/3	Administration	Personnel	Training Plans Investors in People Equal Opportunities	D1 D1 D1	D1 - Destroy locally 1 year after closure.
1/2/1 1/2/2		Management	IM Plan IM Network	D1 D7 RL2	D7 - Destroy 7 years after closure. Retain locally for 2 years then pass to relevant archive.
1/3/1 1/3/2	Information		Asset Registers Maintenance	D15 RL2 D7 RL2	Destroy 15 years after closure. Retain locally for 2 years then pass to relevant archive. Destroy 7 years after closure. Retain locally for 2 years then pass to relevant archive.
2/1 2/2 2/3	Security Equipment	BSO Network Clearances Visits	N/A	D7 PP RL5 D10 RL2	Pass to relevant archive with a recommendation that file part be considered for permanent preservation but retain locally for 5 years.
3/1 3/2	Finance	Budget Structure R&B Policy	N/A	PP RL5 D15 RL2	Destroy 15 years after closure. Retain locally for 2 years then pass to relevant archive.

The above is an example of an extract of a completed retention schedule. In this example, the records are contained in registered files. The schedule must also include any unregistered records.

a. 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).

b. Variations on three abbreviations can be used to record all relevant disposal recommendations:

   (i.) **D** = Retain locally and destroy ‘X’ 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 MOD Archives 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 the relevant MOD Archive for storage or review. (For example file **1/3/1** has been annotated "**D15 RL2**" to denote "to be destroyed 15 years after date of last enclosure but retained locally only for 2 years, after which the file will be forwarded to MOD Archives (e.g. TNT Swadlincote) for storage.").

c. 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 the appropriate MOD Archive 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.

d. 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 Information Manager or 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 5 - Annex C

Ordering Forms from Forms and Publications Commodity Management

5C.1. Corporate Memory, whilst remaining as the Sponsor, has withdrawn its budgetary commitment for all MOD forms relating to paper records management to ensure that business units are accountable for the effective use of the MOD resource. The affected forms are listed in the following table.

FORM	FORM DESCRIPTION
MOD 0001	Document Location Slip
MOD 0057A	Atomic File Cover – Top Secret
MOD 0057B	Atomic File Cover – Secret
MOD 0057C	Atomic File Cover – Confidential
MOD 174A	Temporary Enclosure Jacket (TEJ) – Top Secret
MOD 174B	Temporary Enclosure Jacket (TEJ) – Secret
MOD 174C	Temporary Enclosure Jacket (TEJ) – Confidential
MOD 174D	Temporary Enclosure Jacket (TEJ) – Restricted/Unclassified
MOD 262	Binder for 262A
MOD 262A	File Record Sheet
MOD 262F	Registered File Disposal Form
MOD 329A	Registered File Cover – Top Secret
MOD 329B	Registered File Cover – Secret
MOD 329C	Registered File Cover – Confidential
MOD 329D	Registered File Cover – Restricted/Unclassified
MOD 334A	Personal File Cover – Personal File
MOD 334B	Personal File Cover – Staff Reports
MOD 334C	Personal File Cover – Medical Papers
MOD 334D	Personal File Cover – Disciplinary Papers
MOD 334E	Personal File Cover – Superannuation Papers
MOD 334F	Personal File Cover – Personal File

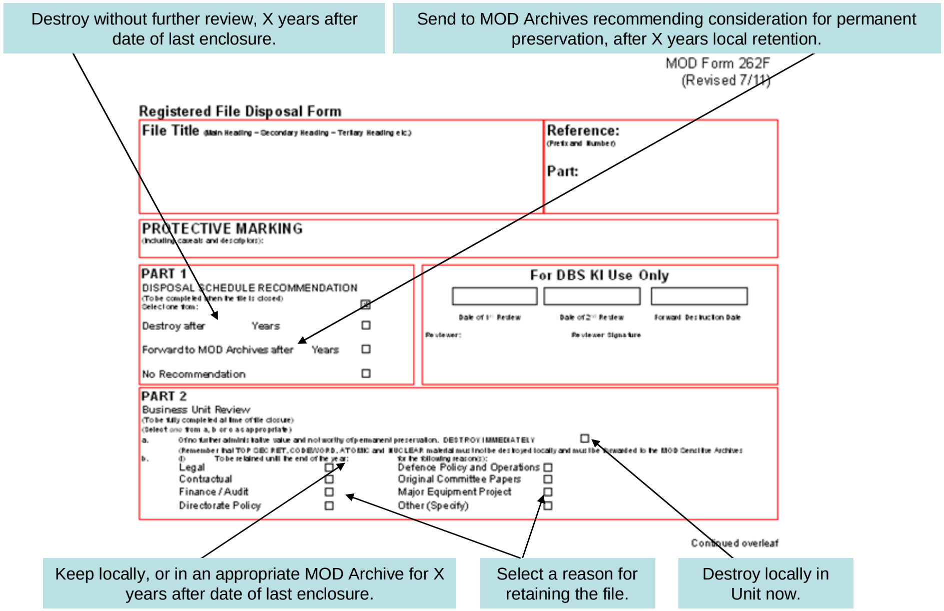
5C.2. To order more forms, business units will need to submit their own requisitions directly to Forms and Publications Commodity Management, using MOD Form 999. Details of the ordering process can be found in DIN 2008DIN04-049. The costs will be charged directly to the requestor's UIN.

5C.3. MOD Form 262A and MOD Form 262F are both available on Defence Intranet.

CHAPTER 5 - Annex D

Completing the Registered File Disposal Form

The following sample MOD Form 262F has some useful tips on completing the form correctly.



Destroy without further review, X years after date of last enclosure.

Send to MOD Archives recommending consideration for permanent preservation, after X years local retention.

MOD Form 262F
(Revised 7/11)

Registered File Disposal Form

File Title (Main Heading – Secondary Heading – Tertiary Heading etc.)

Reference: (Prefix and Number)

Part:

PROTECTIVE MARKING (Including caveats and descriptors):

PART 1
DISPOSAL SCHEDULE RECOMMENDATION
(To be completed when the file is closed)
Select one from: ☒

Destroy after Years □

Forward to MOD Archives after Years □

No Recommendation □

For DBS KI Use Only

Date of 1st Review

Date of 2nd Review

Forward Destruction Date

Reviewer:

Reviewer Signature

PART 2
Business Unit Review
(To be fully completed at time of file closure)
(Select one from a, b or c as appropriate)

a. Of no further administrative value and not worthy of permanent preservation. DESTROY IMMEDIATELY □
(Remember that TOP SECRET, CODEWORD, ATOMIC and NUCLEAR material must not be destroyed locally and must be forwarded to the MOD Sensitive Archives

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

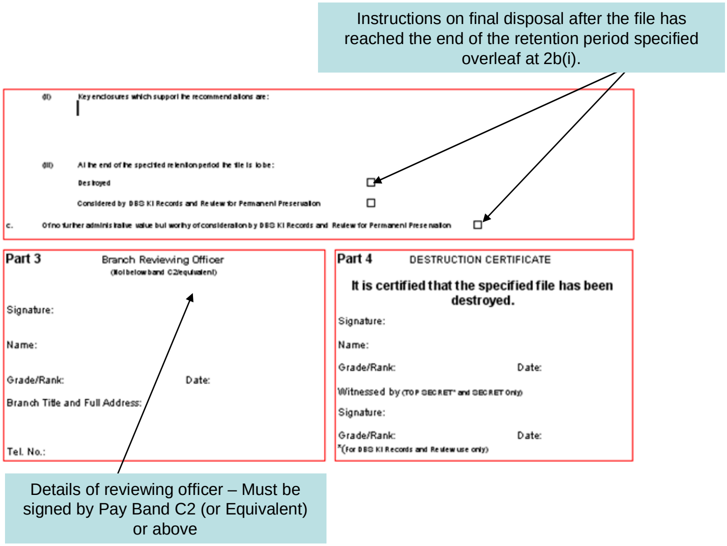
Legal	□	Defence Policy and Operations	□
Contractual	□	Original Committee Papers	□
Finance / Audit	□	Major Equipment Project	□
Directorate Policy	□	Other (Specify)	□

Continued overleaf

Keep locally, or in an appropriate MOD Archive for X years after date of last enclosure.

Select a reason for retaining the file.

Destroy locally in Unit now.



Instructions on final disposal after the file has reached the end of the retention period specified overleaf at 2b(i).

(ii) Key enclosures which support the recommendations are:

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

Destroyed □

Considered by DBS KI Records and Review for Permanent Preservation □

c. Of no further administrative value but worthy of consideration by DBS KI Records and Review for Permanent Preservation □

Part 3 Branch Reviewing Officer
(Not below band C2/equivalent)

Signature:

Name:

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:

Grade/Rank: Date:

Witnessed by (TOP SECRET* and SECRET Only)

Signature:

Grade/Rank: Date:

*(For DBS KI Records and Review use only)

Details of reviewing officer – Must be signed by Pay Band C2 (or Equivalent) or above

CHAPTER 6

Video, Film and Photographs (including Operational and Air Reconnaissance)

Introduction

6.1. The policy for all imagery that the UK collects or receives for intelligence purposes, or which is deemed to be of intelligence value: this includes satellite imaging systems (military and commercial) and airborne, ground-based and sea-borne collection systems can be found in JSP 348 - UK Defence Imagery Policy: Regulations For Demanding, Storage, Archive, Retrieval And Imagery Training.

6.2. This chapter is relevant to all business units, including those who produce material of intelligence value, who create moving images on video tape, optical or non-volatile storage media such as Digital Versatile Disks (DVDs) or Secure Digital (SD) Cards and hereafter known as video, films (including Cine and Video Tele Conference Meetings) and still photographs, and describes the correct procedures for their preservation or disposal.

Background

6.3. All videos, films and photographs that are made or sponsored by MOD Divisions, Establishments, Agencies or Service Units are public records as defined by the First Schedule of the Public Records Act of 1958. The Act requires that, except in certain circumstances, public records selected for permanent preservation shall be transferred not later than thirty years after their creation either to The National Archives (TNA) or to such other place as approved by the Lord Chancellor.

6.4. However, given the relatively fragile nature of video, film and photographs, it has been agreed that action to safeguard those worthy of permanent preservation must be taken much earlier, within five years of their creation.

6.5. The Imperial War Museum (IWM) is the approved place of deposit for MOD video, film and photographs of military or defence related interest or the National Film and Television Archive (NFTVA) for other subjects.

6.6. Selected material must be transferred within the specified time limit to one of the approved institutions.

The Imperial War Museum (IWM)

6.7. The Imperial War Museum is the National Museum of Modern Conflict in the United Kingdom. It records all aspects of modern war, including the causes, course and consequences of conflict. Under the Imperial War Museum Acts of Parliament of 1920 and 1955, the Museum is required to record the military, political, social and cultural impact of such conflict on Britain and the Commonwealth, their allies and enemies, reflecting the experience of both the armed services and civilians. The IWM Photograph Archive and the IWM Film and Video Archive have been appointed as places of deposit for government photographs, film and video which relate to subjects within the terms of reference of the IWM under the Public Records Act 1958 Section 4(1).

6.8. To support the preservation of the official imagery in its care, the IWM is licensed by HMSO to reproduce and administer the rights of MOD and other Crown Copyright imagery in its care.

Video and Film Records

6.9. Video is defined as the process of electronically capturing, recording, processing, storing, transmitting, and reconstructing a sequence of visual still images to represent motion. For the purposes of this JSP, 'video' is to be used as the generic term to encompass motion pictures, including using digital techniques.

6.10. Where the term 'film' is used in this Chapter, it is to specifically distinguish a production that has been stored on cellulose material.

6.11. Videos may range from full productions, such as public relations and training, to records of tests, trials, operations, reconnaissance, video teleconferences etc. They may be edited or unedited and of any duration. They may or may not bear a protective marking.

6.12. Each year, any business unit responsible for making or sponsoring a video (for training video see paragraph 6.13) in the preceding year is to forward details to The DBS KI team (see Chapter 2), who will in turn liaise with TNA to identify material which appears to warrant permanent preservation. Selected videos will be transferred to the IWM (for subjects primarily of military interest) or the NFTVA for other subjects.

6.13. Business units responsible for making or sponsoring training videos in the preceding year must forward details to the British Defence Film Library (BDFL). See paragraph 6.34 below for contact details.

6.14. The process for packaging and sending material of this nature to a pre-approved location can be found at Annexes D and E to this Chapter and must be followed.

When to transfer Video or Film Records

6.15. If a Single Service video, film and photography repository exists, then business units are to send all video and film material to the appropriate repository prior to selection. It will be at this repository where selection will take place and the repository will be responsible for the transfer of selected material to IWM or NFTVA. If this repository does not exist, then selection will take place at the business unit. Business units must contact their relevant Service Historical Branch or for the Army and civilian establishments, the DBS KI team for more details.

6.16. Video or film selection will determine: material that is required for continuing business needs, for example for commercial exploitation purposes, and hence should remain with the business unit; and material that can be transferred immediately to the IWM or NFTVA. Material retained by business units must be transferred to IWM or NFTVA within five years after creation.

6.17. Video or film record selection will take place two years after creation. Business units involved in the selection of material for preservation must seek guidance from their single Service Historical Branches or for the Army and Civilian establishments, the DBS KI team.

6.18. Once selection has been confirmed by the appropriate single Service Historical Branch or the DBS KI team and TNA, then subject to sensitivity (see Annex B), selected master copies will be transferred to the IWM or NFTVA. This transfer is to be as soon as possible after the selection has been confirmed by the DBS KI team and no later than **five** years after creation if the business unit has identified that material needs to be retained for continuing business need. The appropriate single Service Historical Branch or the DBS KI team will inform the recipient of selected material at the time of selection confirmation.

6.19. Material of a sensitive nature **MUST** be forwarded to the DBS KI team once there is no further business need for the material or no longer than twenty five years after creation. If a business unit decides to keep this sensitive material for longer than five years, then they will be responsible for the on-going preservation of the material until its transfer to the DBS KI team (see Annex B).

What should be transferred?

6.20. The master copy of a video or film is to be transferred. The master copy of a video will, for example be either the original tape or a broadcast standard duplicate. In the case of film, the master copy will be either the original negative or a good quality duplicate negative, fine grain positive etc. A viewing copy of the material must be transferred with the master. When material is produced in different formats it is important to forward both a master and viewing copy of each format.

6.21. The transferred video or film must be accompanied by metadata and/or any documents relating to its production for example scripts, shotlists etc., where available.

6.22. Business units may retain copies of the master after five years if there is continuing business need to do so.

Where to send Video or Film Records

6.23. Video selected for permanent preservation at the IWM must be forwarded only after contact has been made to arrange the transfer. See Annexes D and E for more details.

Still Photographs and Micro Film

6.24. Each business unit holding still photographs and micro film is responsible for deciding whether they are of sufficient historical interest to merit permanent preservation. Service personnel involved in this selection process should seek guidance from their single Service Historical Branches. To assist in this task, the following guidelines are to be used (and ANNEX A to this Chapter):

- Age of material – Material should normally be retained for 2 years before it is considered;
- 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 are acceptable. For digital photographs see Annex D for more advice. All material should be accompanied by some kind of supporting documentation.

6.25. These instructions do not apply to photographs or micro film that forms an integral part of a registered file or which provides the supporting evidence to a Board of Inquiry. Such photographs are not to be removed from the file and will be reviewed in the normal way.

Hazard Warning

6.26. Any business unit retaining material on 35mm film which appears to date from 1952 or earlier **MUST** isolate the film or photographic negative. Such film is likely to have been printed on cellulose nitrate stock and constitute a very serious fire and health and safety hazard.

6.27. Acetate film, produced from the 1930's to the 1970's, may suffer from Vinegar Syndrome which is the odour created by decomposing film producing acetic acid. This contaminates other material, is a health and safety risk and the film must be placed in quarantine.

6.28. In both cases and as a matter of urgency, contact the relevant Archive of the IWM (020 7416 5289/5331) for advice.

6.29. In all instances, contact the DBS KI team.

Where to send Non Digital Photographs

6.30. Non digital photographs selected for permanent preservation at the IWM must be forwarded only after contact has been made to arrange the transfer. See Annex E for more details.

Digital Photographs

6.31. The term digital photograph includes all forms of still digital images either taken with a digital camera or taken with a conventional wet film camera and subsequently scanned. Annex C sets out the minimum standards for digital photographs taken for general use throughout MOD.

Where to send Digital Photographs

6.32. Annex D which describes the minimum standards required for metadata, and the subsequent transfer of digital material selected for permanent preservation to IWM, **MUST** be followed.

Presentation to Museums

6.33. If it is considered that any video, film or photograph not selected for permanent preservation by MOD and TNA, may nevertheless, be of value to a museum or other institutions (which may include the IWM in its status as the National Museum of Modern Conflict), then full written details of the nature of the material concerned must be forwarded to Corporate Memory Records DepHd (see Chapter 2). If appropriate, Corporate Memory will seek approval from the Lord Chancellor in accordance with Section 3(6) of the Public Records Act 1958, for the Presentation of the material to the relevant museum or institution.

6.34. Video or film of a training nature **MUST** be sent to:

- BDFL CUSTOMER SERVICES
  British Defence Film Library
  Chalfont Grove, Narcot Lane
  Chalfont St Peter
  Gerrards Cross, Bucks
  SL9 8TN

Contact details:

- Telephone: (Civ): 01494 878278 or Mil: 95298 2278
- Email: BDFL-CUSTOMERSERVICEEMS.WAC@mod.uk

6.35. Video, film or photographs not selected for permanent preservation or Presentation to a relevant museum **MUST** be destroyed when no longer needed for official purposes.

6.36. Corporate Memory Records DepHd **MUST** be advised in writing of any case in which the material is still required by the business unit 25 years after its creation.

Chapter 6 – Annex A

Microform Records

6A.1. The term ‘microform’ includes micro film, microfiche and other similar formats, such as aperture cards, jacketed fiche and blipped film.

6A.2. As far as possible microform records should be passed to the DBS KI team in the original negative form along with a silver nitrate copy and should conform to BS 5699.

6A.3. The following storage conditions are recommended:

- temperature 16°C to 20°C
- relative humidity - Acetate 15 to 40%
  Polyester 30 to 40%

Rapid changes in environmental conditions should be avoided.

6A.4. There may be occasions when only part of a micro film or microfiche might be worthy of permanent preservation (for example, where a micro film consists of copies of a number of registered files). In those circumstances, the whole film or fiche should be forwarded with a covering note identifying the files which are recommended for permanent preservation.

6A.5. To enable individual documents to be identified, each micro film and microfiche must have some indication of its contents and each frame must be numbered (foliated).

6A.6. 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). This should be carried out as normal practice during initial filming operations.

6A.7. If you require further advice regarding microform records please contact the DBS KI team.

Chapter 6 – Annex B

Sensitive Image Records

6B.1. 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).

6B.2. Imagery selected for preservation but which still merit a security protective marking must not be transferred to the Place of Deposit / Presentation until the need for that marking ceases. This sensitive material **MUST** be forwarded to the DBS KI team for storage in the appropriate archives.

6B.3. Business units **MUST NOT** forward sensitive material to the DBS KI team without prior consultation. When agreement is given, then the following is to apply:

Digital Material

6B.4. Sensitive digital material being deposited to the DBS KI team must contain the following overview information:

- The delivery mechanism: for example Portable hard disk drive with FireWire connector.
- How the material is organized: for example 12 folders; HQ LAND output January – December 2007; labelled according to month, with subfolders for Raw, Processed, Photographers Best, etc.
- The approximate number of image files and server/storage space occupied: for example 11.32 GB with 14,000 image files.
- The number of versions of each image, their formats and average image size: for example 3 versions comprising Raw, Worked (processed for web JPEG, PDF); Average file size 6-8 Mb.
- The format, size and coverage of any accompanying metadata: for example 1 CD containing MS Access database containing Tasking data for January – December 2007.
- Any Freedom of Information (FOI) exemptions or Data Protection Act (DPA) restrictions.

6B.5. Any transfer of sensitive digital material must be accompanied by a task listing or a declaration of all the files/images being supplied. This declaration should be in both electronic (MS Word or Excel) format and hard copy. Business units can use a locally produced version of the declaration form at Annex D - Appendices 3 and 4 for this purpose. **Do NOT send a copy of the listing to the IWM**. The hard copy will be used by the DBS KI team to assist their investigation of any missing items from the consignment (i.e. where media has been lost in transit) or to determine which image they have found to be unreadable.

Non Digital Material

6B.6. Non digital material comprises wet process photography and cine film and must be packaged within boxes of archival standard.

6B.7. Within the archive box, photographs (whether negative or print) must be individually enclosed within photographic envelopes, each envelope marked with an identifying number or text.

6B.8. Individual videos must be marked likewise, on the video-sleeve/box and also on the video cassette/cine-reel itself.

6B.9. 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

6B.10. The archive box must be marked externally with the following:

- "Image records for sensitivity re-review"
- the source of the imagery (for example business unit name)
- the earliest recommended review year on the consignment instruction
- the highest protective marking applicable to the contents

6B.11. A second copy of the consignment instruction must accompany the archive box.

Dispatch

6B.12. Sensitive digital imagery and archive boxes containing sensitive non-digital imagery must be sent, in accordance with appropriate JSP 440, Part 5 – Section 3 procedures to:

– DBS KI
1st Floor, Building 2/003
Gloucester Road
HM Naval Base
Portsmouth
PO1 3NH

– Telephone (Mil): 9380 25252

– Telephone (Civ): 023927 25252

Validation

6B.13. The DBS KI team will identify and manage any anomalies found in the sensitive material deposited prior to transfer to their archive. If anomalies are discovered, then the DBS KI team will contact the business unit regarding the queries that they may have on the material.

6B.14. Once this validation process is complete the DBS KI team will send an e-mail confirming the successful transfer and validation of the sensitive material to the named e-mail address identified in the declaration form (See Annex D, Appendices 3 and 4 as appropriate) – **Do NOT send a copy of the listing to the IWM**.

6B.15. Business units must not dispose of their sensitive digital imagery until the DBS KI team has confirmed that the material has been successfully transferred to their digital Archive.

Chapter 6 – Annex C

Minimum Standards for Digital Photographs

6C.1. Originators of digital images should be aware that in addition to the security requirements that apply to the images as official documents, the production of digital images has IT security considerations. For further information please refer to JSP 440, Part 8 - Section 5: Communications Security, Chapter 5: Image Security.

Camera Guidance

6C.2. Cameras with integral combined optical and digital zoom systems should be used with care. Digital zoom simulates optical zoom by enlarging a portion of the image. The effects of digital zoom may lead to the pixilation of the resultant images and a subsequent loss of image quality. Where possible restrict the use of integral zoom lenses to the optical sector only.

Image Formats

6C.3. Although offering many potential advantages there are several issues which affect the use of digital photographs:

6C.3.1. **Memory size and image format** – Raw photographic images can be extremely large. To conserve storage space and reduce transmission time formats have been developed to compress graphical images while still maintaining an acceptable level of detail in the compressed image. The choice of format depends on the type of graphical image and its characteristics (for example amount of detail, the number of colours, and complexity of image).

a. The **Joint Photographic Experts Group** (JPEG) standard is the most commonly used format for displaying pictures in web pages. JPEG image files can typically be one tenth of the size of the original but this reduction is made at the expense of some detail and for this reason JPEG compression should be used warily if the image may be required at a large size for print or examination in the future. JPEG is generally not regarded as an ideal format for long-term preservation.

b. The **Tagged Image File Format** (TIFF) does not lose information and has been developed to operate across a spread of applications and hardware.

6C.3.2. TIFF is currently the most stable means of archiving digital images and must be used whenever possible.

Off-Line Storage Media

6C.4. Currently the most common storage device for photographic images is the CD-ROM (Compact Disk - Read Only Memory). A single CD-ROM at 650Mb could hold several thousand JPEG images at a suitable size for PowerPoint presentations but considerably less if the images are saved at a size suitable for quality reproduction. The CD-ROM is likely to be succeeded by the Digital Versatile Disk (DVD) and in its turn the DVD will undoubtedly be succeeded by a yet more compact, more versatile media such as Blu-ray DVD. However, none of these media offers a reliable means of preserving digital images beyond about 10 years and image libraries on CD or DVD will need to be regularly refreshed to ensure their longevity.

Metadata[16]

6C.5. To realise the full value of digital photographs as records, it is essential that accurate descriptive information (metadata) is created at source. It is also essential for record keepers to know whether an image has been manipulated in any way as this can seriously affect its authenticity.

6C.6. Metadata is the non-image data stored with the image so that it can be reliably retrieved from a large picture library, interpreted correctly and used with confidence. Photographs without basic caption information may become useless with the passage of time and cannot be effectively preserved.

6C.7. It is likely that the range of metadata collected automatically and manually on the camera itself will increase as the technology develops allowing photographers to input metadata immediately.

[16] See also the MOD Metadata Standard (MMS) and JSP 717: Using the MOD Metadata Standard

Chapter 6 – Annex D

Transfer of Digital Material Selected for Permanent Preservation

Introduction

6D.1. To ensure that best practice for the management and long term preservation of digital material is followed, this Annex is governed by the following internationally recognized standards and covers those actions required of the depositing business unit leading up to the transfer of selected digital material to the IWM:

- ISO 14721:2003 – Open Archival Information Systems Reference Model (OAIS)
- ISO 20652:2006 – Producer – Archive Interface Methodology Abstract Standard (PAIMAS)
- ISO 15489:2001 – Information and Documentation – Records Management

6D.2. Adherence to this JSP will lead to a reduced workload for both the depositing business unit and the IWM and will have a positive consequence on the quality of the archived material.

General Guidelines

6D.3. The transfer of any selected (non-sensitive) digital material to the IWM must be carried out with the prior approval of the DBS KI Records Review team. Business units wishing to transfer digital material must complete and submit the declaration form at Appendices 3 and 4 as appropriate, whereupon a review of the material will be performed by the DBS KI Records Review team.

6D.4. To fully satisfy the transfer requirements of digital material to the IWM, those business units depositing material should be aware of and follow the general guidelines listed below:

- Unmanaged digital media has a life of around five years, so do not let backlogs accumulate. The IWM will receive material that is beyond five years old, but only if it is maintained to digital preservation standards. The ideal would be to aim to submit material at quarterly or six monthly intervals to keep the transfer task manageable. IWM advice should always be sought when addressing backlogs of material (generally three or more years' worth of material).
- Ensure that the data is platform independent for example open source formats.
- Avoid submitting files that are too small for archiving, for example web thumbnails.
- Ensure that metadata complies with the MOD Metadata Standard and that the chosen image identifiers are unique. See below for more information.
- Ensure that any FOI exemptions / DPA restrictions are clearly identified and comply with MOD guidelines.

- Ensure that acronyms and abbreviations are intelligible and consistent.
- Ensure that keywords are used.
- Ensure that tasking or declaration information is accurate and available in both electronic and hardcopy form.

Metadata

6D.5. Prior to deposit with the IWM, business units need to be aware of some general points regarding the application of metadata to their digital collections.

- File names and file identifiers – The IWM receives material from all three Services as well as other MOD establishments therefore it is most important that the business unit identifier is unique within MOD. Business units should use their Electronic Unit Name.
- The metadata should relate to what image actually shows.
- Metadata should include: who[17] (subject to DPA restrictions), what, where, when and why (if possible).
- Metadata should be entered in both the raw[18] and worked[19] version of an image – not doing so will prevent a search engine from finding it. Note that the IWM's database system is capable of searching and displaying the contents of the image's metadata fields.
- Metadata that is entered with the image may be published.
- In group shots[20], name the group and the most important individuals for example Officer Commanding, Group Chairman, etc.
- Portraits of unidentified people are unsuitable for archiving purposes even if the party they are part of is known.
- Presentations – Ensure that the award, the Officer making the presentation and the recipient of the award are all clearly identified.
- Always check metadata spelling for typing errors.

[17] To comply with the Data Protection Act, all selected material, other than Public Relations material, where consent has been withheld or has not been obtained, may still be transferred to the IWM but will remain **closed** for 100 years from date of birth.

[18] Raw image: A digital image in its original state without any form of processing being done on it, i.e. downloaded straight from a scanner or camera. This is considered as being the digital negative.

[19] Worked image: A digital image that has been processed using imaging software. This is considered as being a digital print.

[20] In controlled environments such as a photographer's studio, consent must be sought from participants acknowledging that selected material may in future go into the public domain.

- Descriptions, acronyms, abbreviations, etc. must be intelligible and consistent and avoid using terms examples of which are below:
    - Mug shots
    - Interiors/exteriors
    - Royal visit
    - Funeral
    - SCC Group
    - X2 Portrait
    - PERRAS
    - Local children[21]
    - OC
    - The Boss
    - FNG
    - Ops
    - IRT

Complying with the MOD Metadata Standard

6D.6. The MOD Metadata Standard (MMS) (JSP 717: JSP 717 Using the MOD Metadata Standard)) defines the mandatory and optional metadata to be applied to all information objects (including photographs) generated or stored by the MOD and the Services. The metadata elements defined below are the minimum permissible to conform to the MMS and must be collected for each shot or sequence of shots on the same subject.

- A unique reference system following the pattern:
    - aaaa-yyyymmdd-jjj-nnnn for example LAND-20070314-014-37, where:
        - aaaa indicates the Unit taking the photographs (for example LAND, FLEET, BRIZE etc. Business units **MUST** use their EUN.)
        - yyyymmdd is the year, month and day the image(s) were taken
        - jjj is a Job number allocated by the unit
        - nnnn is the Image number within the job
- The photographer (surname-initials-rank/title)
- The time the image(s) were taken
- A title for the event being shot including a subject category
- Caption information (for example Location, personnel, building, ship, aircraft etc. including appropriate subject keywords)
- The security classification/protective marking (for example RESTRICTED)
- Copyright (Normally ‘Crown’ for photographs taken by MOD staff)
- Whether the image has been processed (manipulated) and in what way.

6D.7. Other metadata elements may be added as required in accordance with the MMS. Metadata should be recorded in Rich Text Format.

[21] For their protection, the IWM will not accept images of children without the requisite completed consent form (select from one of the sample forms available in Appendices 1 and 2).

Identifying the Type of Material Suitable for Archive

6D.8. Business units should be aware that the IWM assume that where consent has been given, it is free to disseminate photographs of MOD or other adult personnel.

6D.9. Any images of adults and children that are to be transferred to the IWM must be accompanied with the requisite consent / release forms (See Appendices 1 and 2 for an example of a consent / release form).

6D.10. Digital material generally falls into three main archiving categories:

- Category A – Essential to retain for archiving.
- Category B – Selective – assessment and review is required.
- Category C – No requirement to retain.

6D.11. As a guide, the following types of work have been assigned to the IWM archiving categories:

ACCOMMODATION	(CATEGORY B)
CEREMONIAL	(CATEGORY A)
CHARITY	(CATEGORY B)
CHILDREN	(CATEGORY B)
EXERCISES	(CATEGORY A)
EQUIPMENT	(CATEGORY A)
HOMETOWN	(CATEGORY C)
OPERATIONS	(CATEGORY A)
PARADES	(CATEGORY B)
RECRUITMENT	(CATEGORY B)
SOCIAL	(CATEGORY C)
SPORTS	(CATEGORY C)
STUDIO PHOTOGRAPHY	(CATEGORY B)
PORTRAITS	(CATEGORY B)
PRESENTATION: MEDALS	(CATEGORY B)
PRESENTATION: OTHERS	(CATEGORY B)
UNITS	(CATEGORY B)
VISITS DIPLOMATIC	(CATEGORY C)
VISITS POLITICAL	(CATEGORY C)
VISITS ROYALTY	(CATEGORY A)
VISITS SERVICE	(CATEGORY B)
VISITS VETERANS	(CATEGORY B)
VISITS OTHER	(CATEGORY B)

6D.12. Photographers must include these categories as keywords to their image metadata to assist efficient retrieval and archiving.

Transfer of Digital Material

6D.13. All material selected by MOD and TNA for permanent preservation under the Public Records Act and accepted by the IWM has Public Record status. Business units should also note that the IWM have delegated authority to administer Crown Copyright to any material they receive.

6D.14. So that MOD can fully exploit the potential value of its digital material, business units:

- Are to consider passing, where practicable, a copy of all selected video material to the BDFL.
- **MUST** forward ALL their selected digital photographs to Director Media and Communication (DMC).

6D.15. BDFL and DMC will act as focal points to facilitate the further re-use of this material.

Packaging Information

6D.16. Business units must provide the following overview information of the digital material to be deposited:

- The delivery mechanism: for example Portable hard disk drive with FireWire connector.
- How the material is organized: for example 12 folders; HQ LAND output January – December 2007; labelled according to month, with subfolders for Raw, Processed, Photographers Best, etc.
- The approximate number of video and/or image files and server/storage space occupied: for example 11.32 GB with 14,000 image files.
- The number of versions of each video / image, their formats and average image size: for example 3 versions comprising Raw, Worked (processed for web JPEG, PDF); Average file size 6-8 Mb.
- The format, size and coverage of any accompanying metadata: for example 1 x CD containing MS Access database containing Tasking data for January – December 2007.
- Any FOI exemptions or DPA restrictions in accordance with MOD guidelines.

6D.17. Any transfer of digital material (for sensitive material, see Annex B) must be accompanied by a task listing or a declaration of all the files/images being supplied. This declaration should be in both electronic (MS Word or Excel) format and hard copy. The hard copy will be used by the IWM to assist their investigation of any missing items from the consignment (i.e. where media has been lost in transit) or to determine which image they have found to be unreadable. The IWM pastes the electronic declaration into their record of transfer database system.

6D.18. This declaration ultimately allows the IWM to provide the depositing business unit with rapid acknowledgement of receipt and subsequent validation of the integrity of the deposited material.

6D.19. When declaring the material to be deposited at the IWM, business units **MUST**:

- Reproduce locally, amend and then use the declaration form at Annex D – Appendix 3 for digital images or Annex D – Appendix 4 for digital video, ensuring that the form accompanies the consignment.
- Keep a copy of the declaration form for their records in the event of FOI or other access queries.

- Send a copy of the declaration form to DBS KI.
- (For digital photographs) send a copy of the declaration form to IWM.
- Ensure that image files are readable by using open source formats and that image file naming and associated metadata are consistent and comply with JSP 717: Using the MOD Metadata Standard.
- Deposit digital files in both raw and processed (worked) formats for example TIFF or JPEG, ensuring that where appropriate, each format type is placed in separate folders.
- Consider the following points when transferring their material:
    - For more than 1000 images, units should download the images directly to a portable hard or flash drive using FireWire[22] or USB connectors. The IWM will bear the expense of returning these drives to the depositing unit.
    - For less than 1000 images: CD or DVD is acceptable, however potential depositors should be warned that optical disks are an unreliable form of delivery.
- Submit copies of the completed declaration listing (Appendices 3 and 4) in both hard copy and electronic form with appropriate contact details including a civilian e-mail address and/or phone number.

Where to Send of Digital Video

6D.20. Business units **MUST** forward **ALL** their selected digital video to the IWM. Material selected for permanent preservation at the IWM should be forwarded only after contact has been made to arrange the transfer. Depositors should contact:

– Film and Video Archive
Imperial War Museum
Lambeth Road, London, SE1 6HZ

– Tel: 020 7416 5289
– E-mail: kgladstone@iwm.org.uk

Where to Send Digital Photographs

6D.21. Business units **MUST** ensure that **ALL** digital photographs selected for permanent preservation are forwarded to DMC.

6D.22. DMC will select material suitable for commercial exploitation and retain it for this purpose. The master copy of material retained in this way **MUST** be transferred to IWM within five years of its creation to ensure it is preserved correctly. DMC will also copy material suitable for possible future internal and Public Relations use before forwarding to IWM the masters of such images and the remainder of material selected for immediate transfer on behalf of the originating business unit.

[22] This device is similar in action to the USB but operates at speeds up to 2 gigabytes per second using a 6-wire cable. FireWire connectors are fitted on several digital camcorders and other devices that make use of video data.

6D.23. Business units must package their digital photographs as directed in this Annex and send the material to:

- Director Media and Communication
  Defence Imagery
  Level 1, Zone C, Desk 2
  MOD Main Building,
  Whitehall, London
  SW1A 2HB

Contact details:

- Tel: 020 721 86997
- Email: admin@photos.mod.uk

Validation of Deposited Material

6D.24. The IWM must identify and manage any anomalies found in the material deposited with them prior to transfer to their archive. If anomalies are discovered, the IWM will contact the depositing business unit regarding the queries that they may have on the material.

6D.25. Once this validation process is complete the IWM will send an e-mail confirming the successful transfer and validation of the material to the named civilian e-mail address identified in the declaration form (See Appendices 3 and 4 as appropriate).

6D.26. If the material is subsequently found to be unreadable, depositors will be asked to re-supply the material.

6D.27. Depositing business units must not destroy their copy of any deposited material until they have been contacted by the IWM confirming the satisfactory transfer of this material to their Archive.

Annex D – Appendix 1

SAMPLE RELEASE FORM

For Photographic Still and/or Video Imagery of Adults

PLEASE USE BLOCK CAPITALS

Name:

Unit:

Address:

Tel:

Establishment or location for imagery:

Description of Project/Event and proposed use of images:

1. May we use your images in the above project?

Please Circle
Yes / No

Signature ………………………………………………… Date ……………………

To the Head of the education establishment, cadet group or other body attended by the child/young person.

2. Do you have signed prior parental/guardian permission for photography or filming of the individual above?

Please Circle
Yes / No

Signature ………………………………………………… Date ……………………

Please return this form to:

………………………………………………………………………………..

Annex D – Appendix 2

SAMPLE CONSENT FORM

For Photographic Still and/or Video Imagery of Children and Young Persons below the age of 18

PLEASE USE BLOCK CAPITALS

Name of parent/guardian/carer:

Name of child/young person:

Establishment or location for imagery:

Address:

Description of Project/Event and proposed use of the images:

To the Parent/Guardian/Carer:

1. May we use your child's images in the above?	Please Circle Yes / No

Signature …………………………………………. **Date ………………….**

(of Parent/Guardian/Carer)

To the Head of the educational establishment, cadet group or other body attended by the child/young person:

2. Do you have signed prior parental/ guardian/ carer permission for photography or filming of the individual above?	Please Circle Yes / No

Signature ………………………………………….. **Date …………………..**

Please return this form to:

…………………………………………………………………………………………

Annex D – Appendix 3

Declaration of (Digital) Photographs produced during [*year*], by ______[*photographic production Unit*]

Title / TASK NUMBER	Production Date	Subject Matter	Protective Marking	Comments

Point of Contact Details:
Name:
Branch
Address
Telephone:
Email:

Completed forms should be sent to:	
DBS KI Records and Review **Building 2/003** **Gloucester Road** **HM Naval Base** **Portsmouth** **PO1 3NH**	**Head of Collections Management** **Imperial War Museum** **Photograph Archive** **Lambeth Road, London** **SE1 6HZ**
Military: 9380 25252 **Civilian: 02392 725252**	**Tel. No.: 020 7416 5331**
E-mail: **DBSKI-RecordsReview14@mod.uk**	**E-mail: hroberts@iwm.org.uk**

Annex D – Appendix 4

Declaration of (Digital) Video (and Film) produced during ____[*year*], by _______[Video/film *production Unit*]

Title / TASK NUMBER	Production Date	Duration	Subject Matter	Protective Marking	Comments

Point of Contact Details:
Name:
Branch
Address
Telephone:
Email:

Completed forms should be sent to:	
DBS KI Records and Review **Building 2/003** **Gloucester Road** **HM Naval Base** **Portsmouth** **PO1 3NH**	**Imperial War Museum** **Film and Video Archive** **Lambeth Road,** **London** **SE1 6HZ**
Military: 9380 25252 **Civilian: 02392 725252**	**Tel. No.: 020 7416 5289**
E-mail: **DBSKI-RecordsReview14@mod.uk**	**E-mail: kgladstone@iwm.org.uk**

Chapter 6 – Annex E

Transfer of Non Digital Material Selected for Permanent Preservation

6E.1. Non digital material selected for permanent preservation at the IWM should be forwarded only after contact has been made to arrange the transfer. Depositors should contact:

For Video:

- File and Video Archive
  Imperial War Museum
  Lambeth Road, London, SE1 6HZ
- Tel: 020 7416 5289
- E-mail: kgladstone@iwm.org.uk

For Photographs:

- Head of Collections Management
  Photograph Archive
  Imperial War Museum
  Lambeth Road, London, SE1 6HZ
- Tel: 020 7416 5331
- E-mail: hroberts@iwm.org.uk

6E.2. Non digital material must be packaged within boxes of archival standard.

6E.3. Within the box, photographs (whether negative or print) must be individually enclosed within photographic envelopes, each envelope marked with an identifying number or text.

6E.4. Individual videos must be marked likewise, on the video-sleeve/box and also on the video cassette/cine-reel itself.

6E.5. Within each archive box must be placed a consignment instruction giving the following:

- A hardcopy list or declaration form identifying the contents by subject (also by serial number if appropriate). Business units may use a locally produced and amended version of Annex D, Appendices 3 and 4 as appropriate.
- The review decision for each item (i.e. deposit or presentation).
- The institution selected to receive it.

6E.6. The archive box must be marked externally with the source of the imagery (for example the name of the business unit).

6E.7. A second copy of the consignment instruction must accompany the archive box and a further copy sent to the DBS KI Records Review team.

6E.8. The archive box must be sent, in accordance with appropriate JSP 440, Part 5 – Section 3, procedures to the IWM.

Validation

6E.9. IWM must identify and manage any anomalies found in the material deposited with them prior to transfer to their archive. If anomalies are discovered, then they will contact the depositing business unit regarding the queries that they may have on the material.

6E.10. Once this validation process is complete the IWM will send an e-mail confirming the successful transfer and validation of the material to the named e-mail address identified in the declaration form.

CHAPTER 7

Records Review Process

Introduction

7.1. Reviewing our records is an important aspect of maintaining control of our corporate information as this allows us to establish what information needs to be retained whether for short term administrative reasons or for much longer, possibly for permanent preservation.

7.2. Within MOD the Departmental Records Officer (DRO) has delegated the authority to HQ business and service units to initially review their own records. In most cases, this will mean local destruction of those records that are not considered worthy of permanent preservation, or records that cease to have an administrative value.

The Retention Schedule

7.3. Although our records are important assets that help us do our business, it must also be recognised that they cannot all be retained indefinitely. It is important, therefore, that the Information Manager (IMgr) ensures an effective system of review is maintained, through a retention schedule. The retention schedule is used to:

- Help identify an appropriate length of time that each electronic folder and/or registered file should be kept and their ultimate disposal action.
- Ensure that we only hold records for as long as they are needed and enable us to meet our legislative and statutory obligations under the Public Records, Data Protection and Freedom of Information Acts.
- Support accountability by helping to demonstrate that the disposal of records has been carried out according to an agreed policy and under the proper authority.

7.4. The IMgr is responsible for the creation and maintenance of the retention schedule, and co-ordinating the dissemination, of electronic folders and registered files to be reviewed, to the relevant desk officer or subject matter expert. This task involves considering all existing electronic folders and registered files held by the business unit and identifying which category each falls into. For guidance, initial retention periods assigned to these electronic folders and registered files will be those that have been advised by The National Archives (TNA).

7.5. In many cases these recommendations will remain valid even when the existing electronic folder or registered file is closed and a new part opened. For instance, if an electronic folder or registered file has been recommended for transfer to TNA because it illustrates significant developments in an area of policy, it is quite likely that any subsequent part of that electronic folder of registered file will fall into the same category.

7.6. The desk officer or subject matter expert (hereafter known as the Reviewing Officer) is best placed to recommend suitable retention periods based on their working knowledge of the nature and content of the electronic folder or registered file.

7.7. It may be that subsequent parts of an electronic folder or registered file increase or diminish in importance in relation to previous parts. If this were found to be the case then the Reviewing Officer **MUST** advise the IMgr to amend the retention schedule of the electronic folder or Register file accordingly.

7.8. As new electronic folders and registered files (as opposed to new parts of existing electronic folders and registered files) are opened, the IMgr must establish whether an initial recommendation about disposal can be made.

7.9. Annex A to this chapter offers guidance on how long to retain different types of records, and provides examples of records that are likely to warrant permanent preservation.

Eligibility

7.10. Only staff at Band C2 (or equivalent) grade and higher are eligible to undertake these reviews.

The Review for Electronic Folders

7.11. Mechanisms within the ERMS should ensure that folder parts are regularly closed, and that the IMgr and their staff are notified when a folder part is scheduled for review and further action.

7.12. Once closed, all electronic folder parts must be reviewed within the allocated timescales, and the appropriate disposal action carried out.

7.13. When an electronic folder part is due for review, the IMgr must first consider whether the electronic folder is likely to be needed for administrative or historical purposes and whether its original disposal action is still valid. The Electronic Records Folder Review Form at Annex C can be used to assist with this review process.

7.14. Where, for instance, a group of electronic folders contain material of a local administrative nature, this usually indicates that the content of these folders need not be kept beyond the stated review period. These folders can therefore be destroyed locally without seeking additional consent from the Reviewing Officer.

7.15. If it has been judged that a particular folder part contains information that needs to be kept to help progress work with current activities, then the retention period on that particular folder part will need to be increased.

7.16. Electronic folders containing material of a specific nature (for example operational, medical, legislative, scientific, or policy) are to be passed to the Reviewing Officer for review. Initial examination of the folder titles will usually give the reviewer a good indication as to whether its content warrants consideration for retaining beyond its specified initial review period.

7.17. If the initial examination deems that the folder contains records that must be retained, then the records within the folder should be examined more closely to judge whether a further extension to the folder's retention period needs to be applied or the folder is to be permanently preserved.

7.18. Even if only one record is deemed to warrant a folder's retention period being extended while the other records warrant no value at all, since the "weeding" of records is prohibited, the whole folder is to be kept to ensure the information retains its integrity.

7.19. Once the Reviewing Officer is satisfied that an appropriate review has been undertaken and they are in a position to recommend the review decision they must advise the IMgr, in writing, accordingly, so that the IMgr can perform the appropriate disposition.

7.20. Where it has not been possible for the Reviewing Officer to easily determine the disposal action of a folder, then the folder must be retained for an additional period of time with the retention schedule so annotated. The Electronic Records Folder Review Form at Annex C can be used to assist with this process and is available on the Defence Intranet.

7.21. There is no requirement to maintain File Records Sheets (MOD Form 262A) or File Disposal Forms (MOD Form 262F) for wholly electronic folders.

The Review of Registered Files

7.22. When a registered file is closed, a MOD Form 262F **MUST** be raised and placed in the file. To determine the appropriate retention period and method of disposal for the file, the retention schedule must be consulted and used to annotate the MOD Form 262F.

7.23. The IMgr must then consider whether the file is likely to be needed for administrative or historical purposes, as part of the initial review. Additionally, consideration must be given to whether the material continues to merit its original protective marking, or whether it should be downgraded.

7.24. Where a registered file contains material of a local administrative nature, this usually indicates that its content may not need to be kept beyond its stated review period. If the file is then subsequently deemed to have no ongoing administrative value, the IMgr should destroy it locally. The MOD Form 262F must be annotated accordingly, noting the decision taken, and replaces the MOD Form 262A held in the binder relating to the file‘s series. However, if the file has not been destroyed within 25 years of its closure, permission must be sought, in writing and with a suitable justification, from Corporate Memory Records DepHd to retain it further,

7.25. If the registered file contains material of a specific nature (for example operational, medical, legislative, scientific, or policy) this must be passed to the relevant Reviewing Officer for review. Records within the file should be examined to the extent necessary to enable a judgement to be made on whether a further extension to the file's retention period needs to be applied or if the file is to be permanently preserved or destroyed.

7.26. Even if only one record is deemed to warrant a file's retention period being extended while the other records warrant no value at all, as the "weeding" of records is prohibited, the whole file is to be kept to ensure the information retains its integrity.

7.27. If the ultimate recommendation is that the file must be retained for an extended period for administrative purposes, or that the file warrants permanent preservation, the specific enclosures which justify that recommendation (which must be identified on the file minute sheet) must 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 to be identified.

7.28. Once the IMgr or the Reviewing Officer has reviewed the file, the MOD Form 262F must be completed to advise their recommendation for the files disposal.

The Review of Unregistered Material

7.29. 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 the DBS KI Records Review team for permanent preservation should be forwarded in accordance with the instructions at Chapter 8.

7.30. The "Record of Unregistered Material" must also be amended to reflect the disposal recommendation for the unregistered record. Further guidance about how long to keep records can be found at Annex A.

Existing Files Not Reviewed at Time of Closure

7.31. All registered files must be reviewed at the earliest opportunity, and sections 2 and 3 of MOD Form 262F completed. 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.

Retention of Registered Files by the Business Unit

7.32. If the completed and signed MOD Form 262F recommends that the file is to be considered for permanent preservation it should normally be sent to the relevant archive within 5 years of its closure.

7.33. Certain Air Force department files, for example Chief of Air Staff, Vice Chief of Air Staff and RAF Form 540 (Station Diaries), may initially be sent to the Air Historical Branch (RAF) with the prior agreement of both the Air Historical Branch and Corporate Memory.

7.34. To allow a judgement to be made about the historical context of records judged to be worthy of permanent preservation, the DBS KI Records Review team will conduct a review of these files. Files which are selected for permanent preservation are normally passed to TNA and then made available to the public in accordance with the terms of the Public Records Act of 1958 and 1967.

7.35. Files which have ongoing administrative value must be retained locally for an extended period and should be forwarded to the relevant archive when they are no longer needed. However, Corporate Memory Records DepHd 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.

7.36. 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 retained locally. However if local storage space is at a premium, low usage files should be sent to the relevant archive instead. In these circumstances the IMgr must ensure that explicit reasons are given on the MOD Form 262F (and on the business unit’s copy) for the ongoing retention of the file. Failure to do so may result in the file being destroyed by the DBS KI Records Review team.

Retention of Other Records

7.37. Unregistered records which merit consideration by the DBS KI Records Review team for permanent preservation must be forwarded within 25 years of their creation, in accordance with the instructions in Chapter 8.

7.38. 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, in writing and with a suitable justification, from the Corporate Memory Records DepHd to retain them.

7.39. 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.

Maintaining the MOD Form 262A and MOD Form 262F

7.40. The File Record Sheet (MOD Form 262A) and the File Disposal Form (MOD Form 262F) are the definitive record of a file's existence and subsequent destruction/passage to the relevant archive.

7.41. The MOD Form 262A must not be destroyed until replaced by MOD Form 262F.

7.42. 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).

7.43. If MOD Form 262F is retained in a binder relating to a file series or a number of file series, the binder must be retained for a period of not less than 30 years following the insertion of the final MOD Form 262F.

7.44. If a business unit is disbanded during this period, the binder(s) must be passed to the successor business unit. If there is no successor business unit, the binder(s) must be forwarded to the relevant archive.

7.45. When a file is destroyed by the business unit, the MOD Form 262F is to be removed from the file and used to replace the MOD Form 262A which should then be destroyed.

7.46. 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.

Sponsors of Manuals and Books of Reference

7.47. 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 the appropriate archive in accordance with the instructions in Chapter 8.

Destruction of TOP SECRET Registered Files and Files Containing Codeword Material

7.48. All registered files containing TOP SECRET and/or codeword material are to be forwarded to the Sensitive Archive, even if the Registered File Disposal Form recommends that the file should be destroyed.

7.49. 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.

Chapter 7 – Annex A

Types of Records held by Business Units

Type of Record		Retention Period
Administrative		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		Usually defined by an individual's age unless a statutory or a long-term operational requirement defines a period for their continued retention. For example, records relating to criminal investigations or Service Inquiries may be retained, depending on the subject for 75 years or more. (For all types of Inquiry, it is recommended that business units retain copies of all relevant supporting documentation together.)
Command and Control and Operational		Some records in these categories can have a long life span and should be considered for permanent preservation. Corporate Memory Analysis (for the Army and PJHQ) and the other single service Historical Branches (for the RAF, RN and RM) should be consulted on the retention and disposal of operational records.
Estates and Accommodation	Legal	Estate title, leasehold documentation, etc., should be retained for at least the occupancy period.
	Policy	Surveys, policy studies etc., retention varies between 10 to 25 years but records relating to important aspects such as disposal of potentially hazardous substances on sites or other health and safety issues should be kept for much longer periods of time.
Finance		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		Statutory requirements mean that some records can have a very long retention requirement. (NOTE: JSP 375: The MOD Health & Safety Handbook also offers guidance).
Personnel	Pension	Documents that have a bearing on pension entitlement should be kept for 100 years from date of birth.
	Military Personnel	Service personnel appraisal reports are to be kept for 100 years from date of birth.

Type of Record		Retention Period
	Civilian Personnel	Civilian staff appraisal records are to be kept for 10 years as separate sub-sets of personal files. 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 must be kept for 100 years.
Policy		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 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, for example Porton Down records covering the volunteer programme go back to the 1950's.
Transaction		These records record specific events that have a finite life, for example 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.

Chapter 7 – Annex A – Appendix 1

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 marked for retention by them.
- Illustrating the formation / evolution of Defence Policy
- Illustrating significant developments in the relationship between MOD and other organs of government, or other national or international authorities.
- Showing the authority under which MOD has exercised a function.
- That contain important decisions relating to the organisation, disposition or use of the Armed Forces
- Describing 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.
- Reflecting Law Officers' opinion on any subject.
- Setting up, proceedings and reports of committees, working parties and study groups.
- Introducing/considering new types of weapons and equipment.
- Introducing/considering the modification of weapons and equipment.
- Of important trials and exercises.
- Introducing new types of uniforms, clothing etc
- About 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.
- Containing reports of significant operations, intelligence, organisational and logistical matters.
- Of Histories produced by Service units etc.
- Of Standing Orders and similar instructions of Commands, Agencies, Establishments etc.

- Diaries, journals, logs, etc. providing an insight into particular operations or activities of wide interest.
- Containing records relating to famous or infamous people.

Chapter 7 - Annex A – Appendix 2

Guidance on how long to keep records

Contracts

7A.1. 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 1980

7A.2. 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.)

7A.3. Records relating to contracts worth less than £5,000 should be destroyed no later than two years after the end of the contract.

7A.4. 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 TNA.

Accounting Records

7A.5. 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.

7A.6. 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 2006.
- Consumer Protection Act 1987.
- Data Protection Act 1998.
- Financial Services Act 2010.
- Limitation Act 1980.
- Freedom of Information Act 2000.

7A.7. Business units 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.

7A.8. 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 two years has been substituted 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

Building Records

7A.9. This guidance covers all buildings on the Government Estate and is supported by English Heritage (Conservation Unit).

7A.10. 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, for example personnel and wages records. Government building records are varied but, for the purposes of this guidance, are divided into three broad types:

- Legal – These include estate title, leasehold and other contract documentation relating to the building and its surrounding land.
- Policy – These include surveys, evaluation reports, policy studies, etc.
- Administrative – These records are relevant to the maintenance, repair and reconstruction of buildings, and may comprise information such as survey drawings and records of services, historical narratives and descriptions, photographs, inventories of plant, equipment and furnishings and possibly archaeological information about the site and building.

7A.11. When assessing review dates the following principles must be borne in mind:

- The implication of legislation will mean that certain legal records may have to be kept for up to 16 years.
- The potential value of records for the future when maintenance, repair, alteration, etc. of the building is proposed or planned.
- Records which are likely to be of historic value and which may be preserved in TNA include: surveys, project specifications, project board minutes, policy files, planning and other certificates, written accounts of historic buildings, photographic records of maintenance and building, etc.

Health & Safety Records

7A.12. The legislation underpinning health and safety in the United Kingdom is the Health and Safety at Work Act 1974. 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.

7A.13. 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. Health and safety records might be kept for the following reasons:

- The records are required by legislation.
- The operations or process may be used again and the records are needed to ensure safety.
- The records 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.

7A.14. The Management of Health and Safety at Work Regulations 1999 and as amended by the Management of Health and Safety at Work (Amendment) Regulations 2006 requires pre-employment medical screening to determine whether someone can carry out a specific task without risk to their health and safety. These records need to be kept for the duration, and after, the employee has carried out these tasks in case of claim for compensation.

7A.15. Under the Limitation Act 1980, personal injury actions must be commenced within three years of the injury or the date of knowledge of the injury. For example, 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.

7A.16. It is recommended that relevant records be kept for 40 years for such incidents. Evidence that may be useful could include relevant risk assessments for example formal surveys of the workplace, safe operating procedures, effectiveness of controls for example monitoring of noise and/or light levels, maintenance records for machinery and medical surveillance for example pre-employment medicals and audiometry.

7A.17. Records of health and safety, environmental incidents and accidents are to be included on the Incident Recording Information System (IRIS) which now provides a single system for recording and monitoring all safety related incidents and all common law claims.

7A.18. MOD policy on the management and retention of health and safety records for all staff can be found in JSP 375 – Volume 2 – Leaflet 55 – Retention of Records.

Personnel Files

7A.19. The recommended retention period for most records is 100 years from the date of birth. The main reason for this has been the requirements of the Principal Civil Service Pension Scheme (PCSPS).

7A.20. 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 100 years from date of birth or 5 years from last action, whichever is the later.

7A.21. Personal security records should be kept as separate annual sub-sets of personal files. Careful consideration should be made as what personal information is to be held on individuals, with arrangements made to ensure that it is stored securely for as long as is required and no longer (see DPA Guidance Note 5) and then appropriately disposed of.

7A.22. Medical records[23] should be kept as separate annual sub-sets of personal files.

Airworthiness Records

7A.23. Details about Airworthiness records and how long these records should be retained can be found in JSP 553: Military Airworthiness Regulations and its associated publication JAP 100A-01: Military Aviation Engineering Policy and Regulation, Chapter 7.6.

Other types of records

7A.24. Contact the Corporate Memory Records team for guidance on how long to keep other types of records.

Electronic folders

7A.25. Retention schedules are an essential feature of all Electronic Records Management System (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 be assigned to the file plan and hierarchies of folders can inherit these as defaults from higher-level folders.

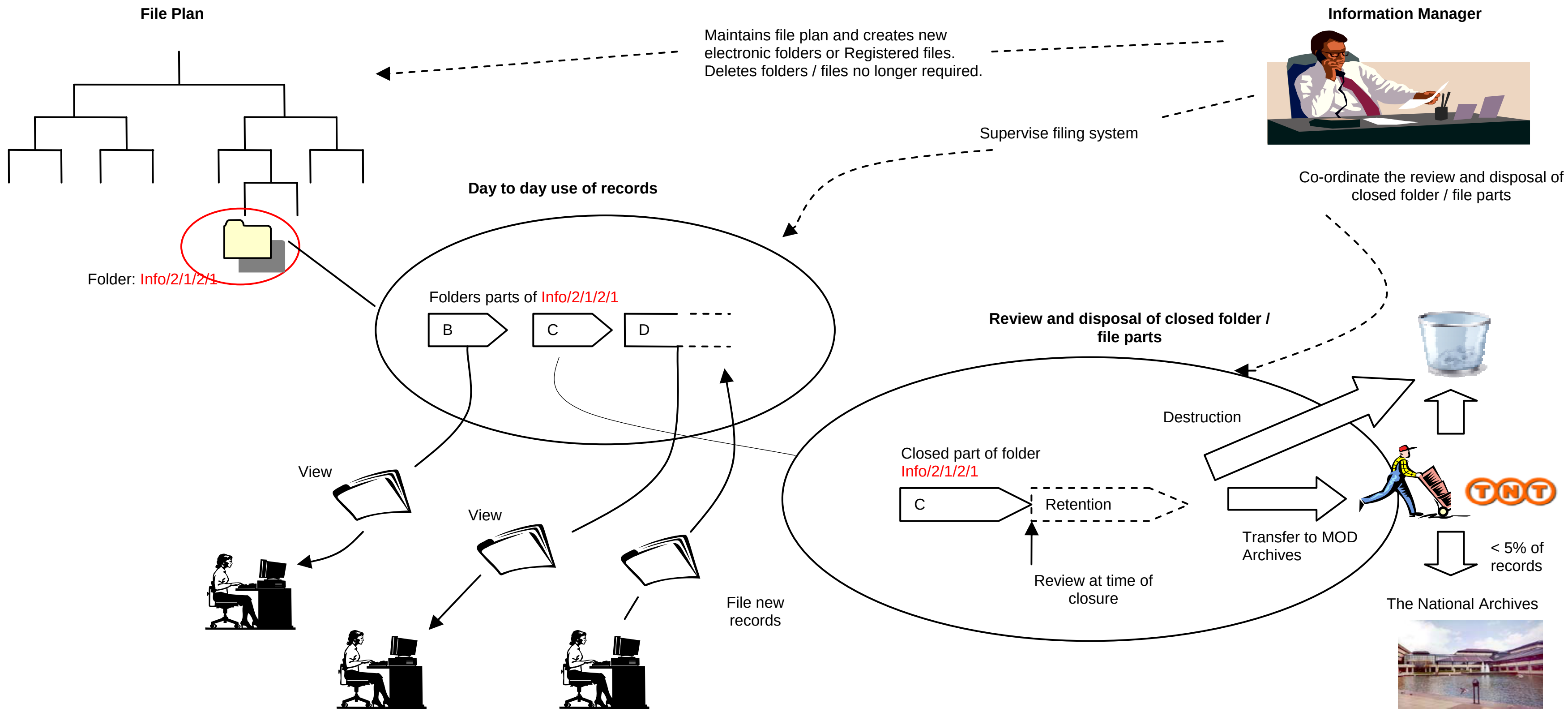
7A.26. Most ERMS will contain a series of pre-defined retention schedules, from which information management staff, in consultation with the Reviewing Officer, can select the most appropriate. If no retention schedules have been defined, iHub staff must contact the Corporate Memory Records team (see Chapter 2) for guidance.

7A.27. It should be noted that in exceptional circumstances, for example where the defined retention schedule is too short, Corporate Memory reserves the authority to override any local decisions.

[23] Departmental health and safety issues potentially affecting multiple members of staff, such as records under: Control of Substances Hazardous to Health (COSHH) regulations, or Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR), should be documented on business unit's administration or subject files (cross-references from these files to those of likely effected staff would be useful).

Chapter 7 - Annex B

Record Management Overview



File Plan

Folder: Info/2/1/2/1

Information Manager

Maintains file plan and creates new electronic folders or Registered files. Deletes folders / files no longer required.

Supervise filing system

Co-ordinate the review and disposal of closed folder / file parts

Day to day use of records

Folders parts of Info/2/1/2/1

B

C

D

View

View

File new records

Review and disposal of closed folder / file parts

Closed part of folder Info/2/1/2/1

C

Retention

Review at time of closure

Destruction

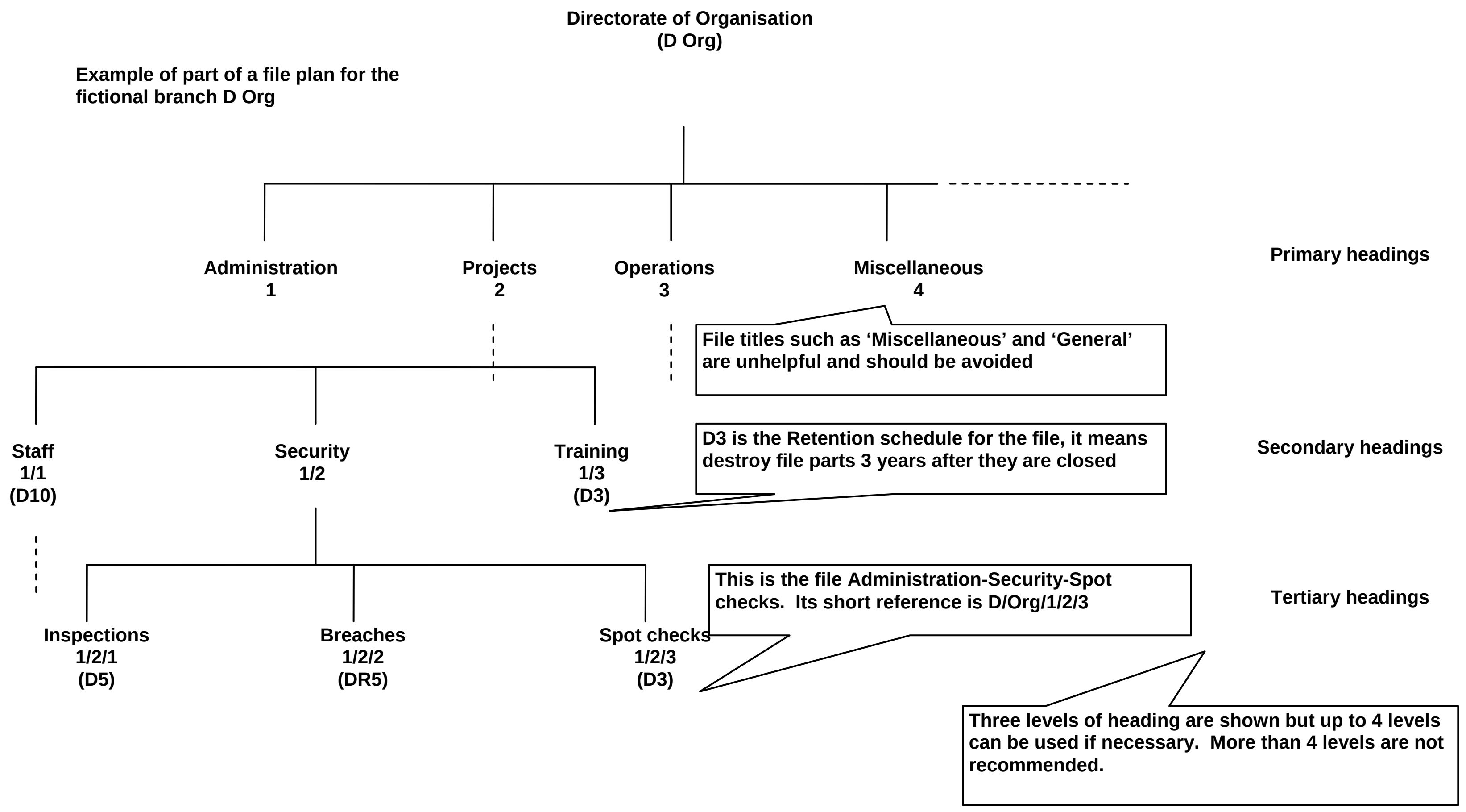
Transfer to MOD Archives

< 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 Information Manager is responsible for creating and maintaining the file plan, ensuring that the filing system is being used correctly, ensuring that electronic folder / file parts are closed and reviewed in a timely manner and disposed of as soon as their recommended disposal period has expired.
- These activities are explained in more detail in the following diagrams.



Directorate of Organisation
(D Org)

Example of part of a file plan for the fictional branch D Org

Administration
1

Projects
2

Operations
3

Miscellaneous
4

Primary headings

File titles such as ‘Miscellaneous’ and ‘General’ are unhelpful and should be avoided

Staff
1/1
(D10)

Security
1/2

Training
1/3
(D3)

D3 is the Retention schedule for the file, it means destroy file parts 3 years after they are closed

Secondary headings

Inspections
1/2/1
(D5)

Breaches
1/2/2
(DR5)

Spot checks
1/2/3
(D3)

This is the file Administration-Security-Spot checks. Its short reference is D/Org/1/2/3

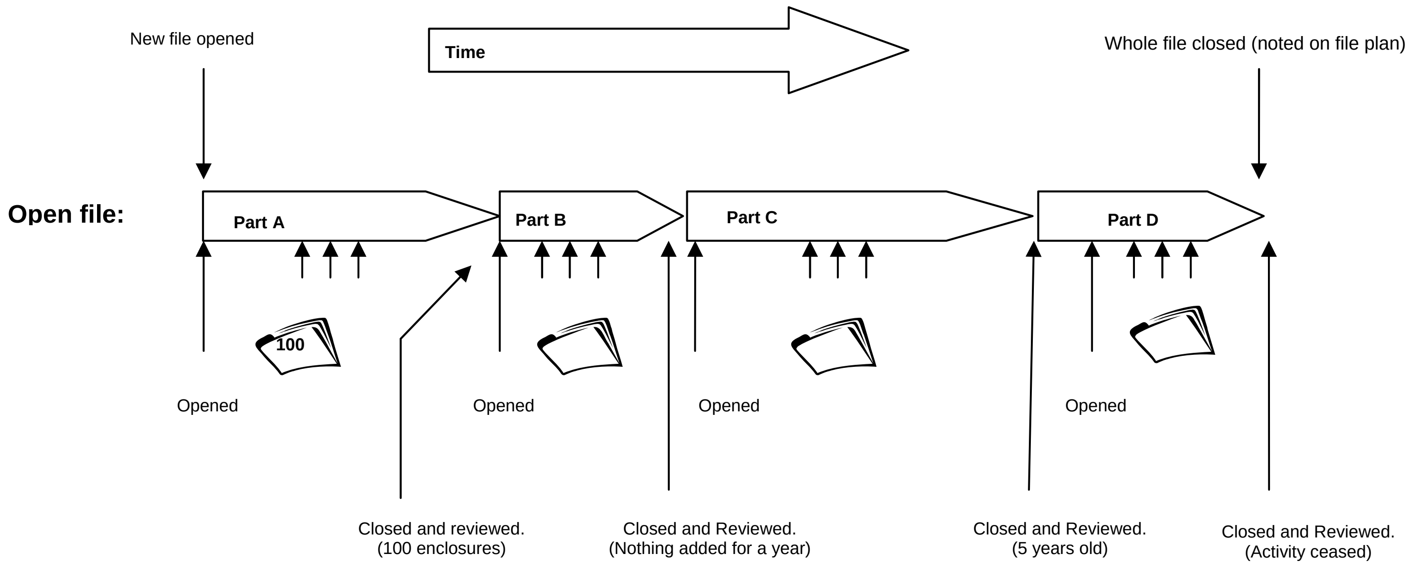
Tertiary headings

Three levels of heading are shown but up to 4 levels can be used if necessary. More than 4 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 must have a numerical reference.
- Each file must have a retention schedule recommendation associated with it to show when file parts should be destroyed or passed to DBS KI for consideration for permanent preservation.
- New file plans must be approved by the Corporate Memory Records team who can also give guidance on construction of file plans.
- Keep the file plan logical and simple.

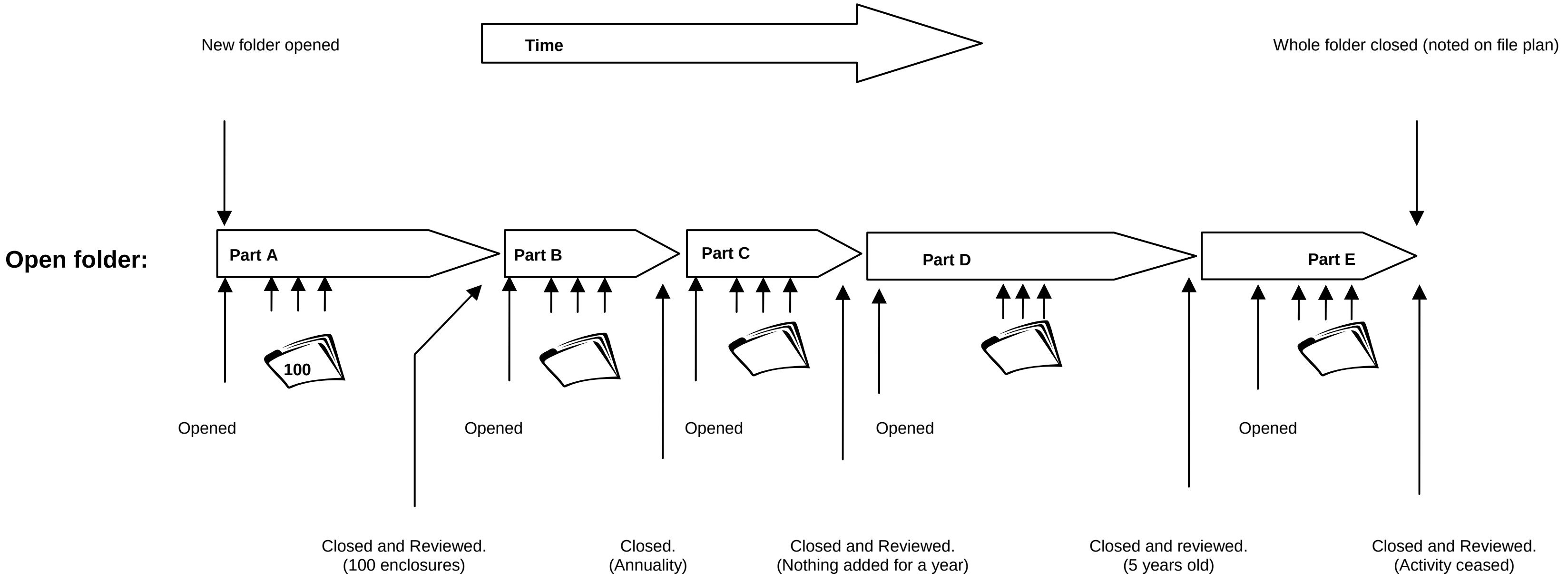
THE LIFE OF A REGISTERED FILE


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 registered file which over time has been 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 AN ELECTRONIC FOLDER

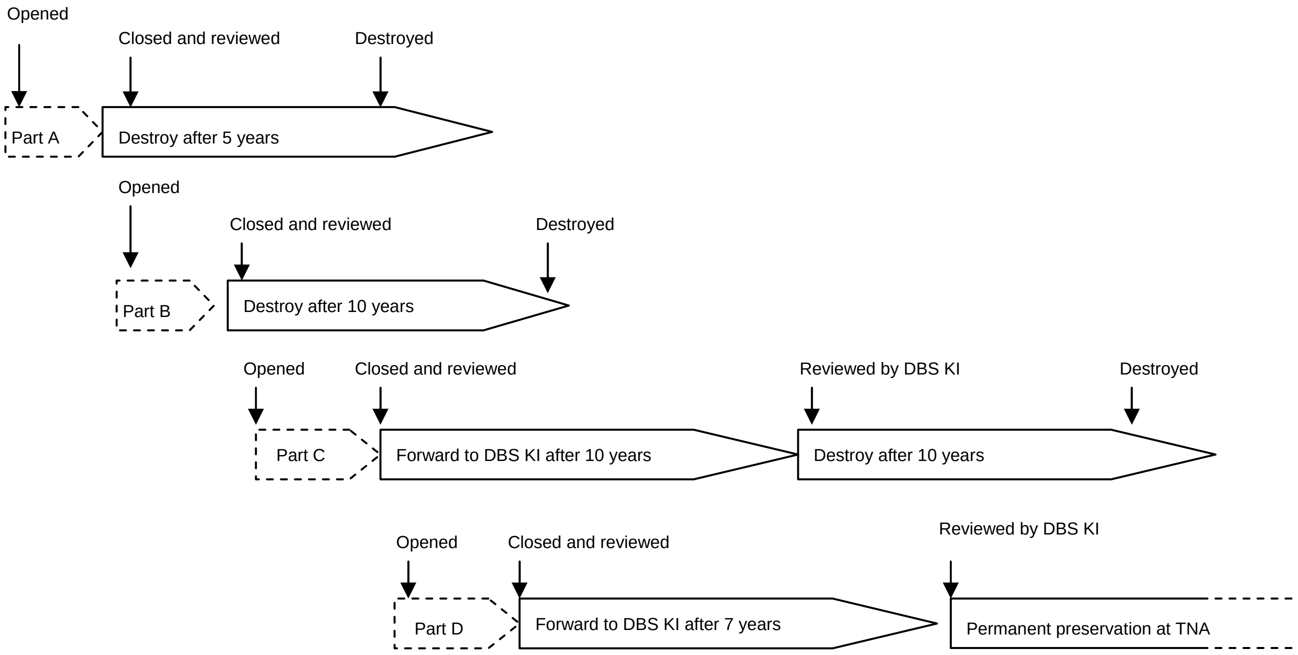


Notes:

- Here is the life-cycle of a typical electronic folder which over time has been split into five parts A, B, C, D and E.
- 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), annuality (Part B), nothing added for a year (Part C), the part is 5 years old (Part D).
- Eventually the activity associated with the folder totally ceases so there is no longer a need for the folder. Its final part (Part E) is manually closed and the whole folder is recorded as closed on the ERMS file plan.

THE LIFE OF A CLOSED ELECTRONIC FOLDER / REGISTERED FILE

Chapter 7 Annex B

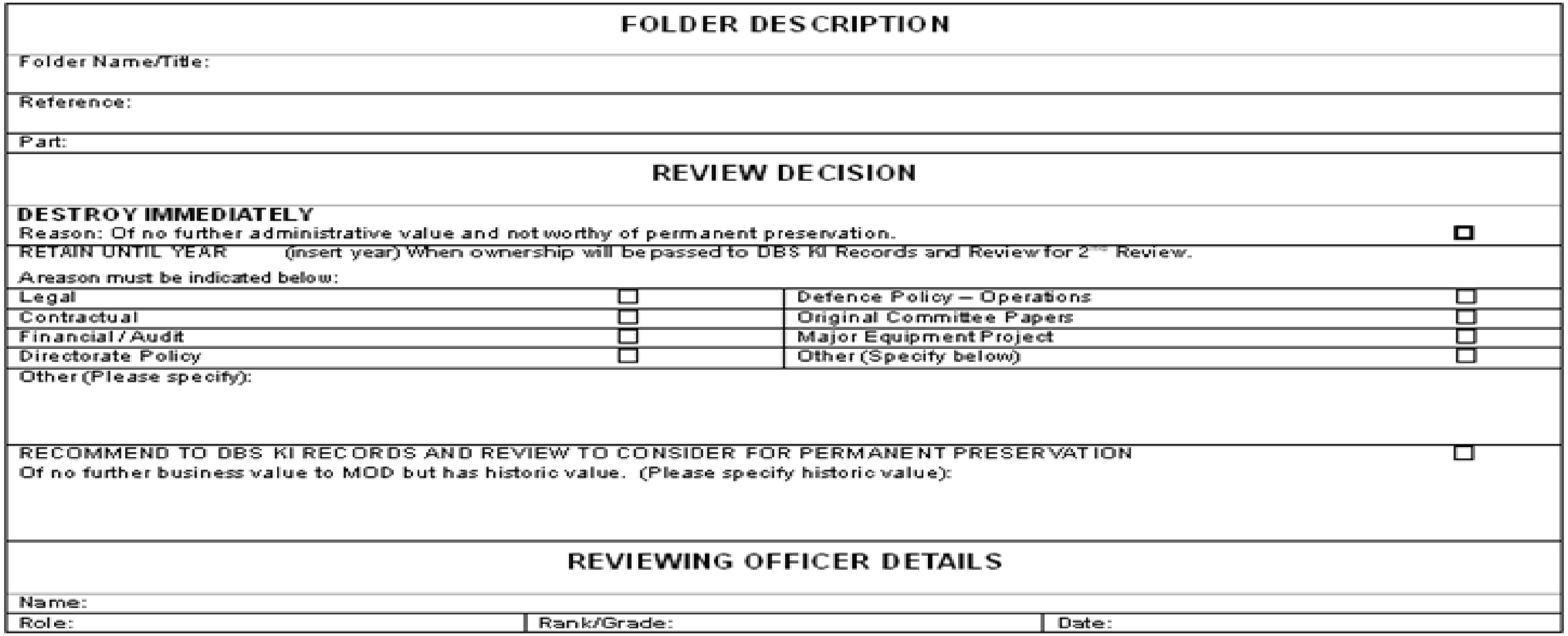


Notes:

- Here is the life-cycle of a closed file. Its retention 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 retention schedule recommendation and is destroyed 5 years after closure.
- At Part B the reviewing officer decides to extend the retention period to 10 years at which point the file part is destroyed.
- At Part C the reviewing officer decides to transfer the file part to DBS KI as it may merit permanent preservation. The DBS KI records reviewer decides that permanent preservation is not merited and marks the file for destruction after a further 10 years.
- At Part D the reviewing officer decides to transfer the file part to DBS KI as it may merit permanent preservation. The DBS KI records reviewer agrees that permanent preservation is merited and arranges transfer to TNA.

Chapter 7 - Annex C

Electronic Records Folder Review Form



FOLDER DESCRIPTION

Folder Name/Title:

Reference:

Part:

REVIEW DECISION

DESTROY IMMEDIATELY

Reason: Of no further administrative value and not worthy of permanent preservation. □

RETAIN UNTIL YEAR (insert year) When ownership will be passed to DBS KI Records and Review for 2nd Review.

A reason must be indicated below:

Legal	□	Defence Policy – Operations	□
Contractual	□	Original Committee Papers	□
Financial / Audit	□	Major Equipment Project	□
Directorate Policy	□	Other (Specify below)	□

Other (Please specify):

RECOMMEND TO DBS KI RECORDS AND REVIEW TO CONSIDER FOR PERMANENT PRESERVATION □

Of no further business value to MOD but has historic value. (Please specify historic value):

REVIEWING OFFICER DETAILS

Name:

Role: Rank/Grade: Date:

(Revised 7/11)

CHAPTER 8

Forwarding Material to MOD Archives

When to Forward Records to MOD Archives

8.1. Records held by MOD HQ and other business units should normally be forwarded to the MOD Main Archive run by TNT Archive Services, or the MOD Sensitive Archive 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 the appropriate archives within 25 years of their closure unless prior written authority has been obtained from CIO-CI-Corporate Memory DepHd to retain them.

8.2. If you plan to send a large quantity of paper records to the MOD Main Archive please contact the Contract Management Team (CMT) first advising the type and quantity of records involved. This will ensure that suitable provision can be made for their arrival. The CMT can be contacted by:

- Email: DBSKI-RecordsCMTMgr@mod.uk
- Telephone: (9)4240 5701 / 01869 259701

8.3. The appropriate MOD Archives should be contacted before unregistered records are forwarded, unless they form part of an existing Special Project agreed with the Contract Management Team.

Closure of Business Units

8.4. When a business unit is due to be closed (or a ship decommissioned) the Information Hub (iHub) must make provision for the appropriate disposal of the records held by that business unit.

8.5. Prior to the closure of the business unit, the iHub must make arrangements for registered files and electronic folders to be reviewed (see Chapter 7). Those files and folders which are no longer required, because they have passed their retention periods and are no longer required for business use and have no historic value should be destroyed.

8.6. Custodianship should be transferred to the successor or parent unit for those electronic folders that need to be retained and funding provision planned for, in those situations where electronic records are to be transferred from one system to another.

8.7. Registered files that need to be retained should either be:

8.7.1. Sent to the MOD Main Archive for up to SECRET material or the MOD Sensitive Archive in Portsmouth for material above SECRET.

8.7.2. Transferred to the successor or parent unit, if still required for business use.

8.8. If records are to be transferred to another business unit action should be taken as detailed in Chapters 4 and 5 of 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 appropriate MOD Archive.

8.9. Where some or all tasks of a business unit are to be transferred to a private contractor, for example its services are contracted out or part or all of the business unit is privatised, then the business unit IMgr is to contact the Corporate Memory Records team at the earliest opportunity for guidance on the review, disposal or potential transfer of these records.

8.10. All business units are required, as part of their planning process, to make funding provision for the movement and archive of paper records. As part of this process, the CMT is to be notified. CMT will provide assistance with the planning and costing of the movement of registered files that are destined for the MOD Main Archive.

Machinery of Government Change

8.11. A Machinery of Government (MoG) change is a transfer of functions between Ministers, either between Ministers in charge of Departments or other Cabinet Ministers, or between a Minister and a non-Departmental public body (NDPB).

8.12. 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.

8.13. Business units affected by a MoG change must have a clear understanding of their roles and responsibilities and will need to work closely with Corporate Memory Records to achieve an effective transfer of their paper and electronic records, as well as informally held information and knowledge.

8.14. Broad guidance on the transfer of records, information and knowledge as a result of a MoG change, can be found on The National Archives website or by consulting Corporate Memory Records DepHd. This guidance is also useful for those personnel who are involved in preparing their business units for closure.

Transfer of Records to The National Archives

8.15. Records which are selected as worthy of permanent preservation are prepared for transfer to The National Archives (TNA) by MOD records and review staff: 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.

8.16. 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. Records with continuing business use can also continue to be held by MOD. However, the Lord Chancellor's approval must be sought in both cases and it is therefore imperative that records which might warrant continued closure or retention, for whatever purpose, are identified to Corporate Memory Records within 25 years of their creation/closure. Any business unit holding records in this category should write to CIO-CI-Corporate Memory DepHd who will provide specific guidance.

Presentation to Museums

8.17. If it is considered that any records not selected for permanent preservation by MOD and TNA, may nevertheless, be of value to a museum or other institutions, then full written details of the nature of the material concerned must be forwarded to CIO-CI-Corporate Memory DepHd. If appropriate, Corporate Memory will seek approval from the Lord Chancellor in accordance with Section 3(6) of the Public Records Act 1958, for the Presentation of the material to the relevant museum or institution.

Sending Records to MOD Archives

8.18. There is more than one destination for records being forwarded to MOD Archives. The appropriate destination is determined by the type of record involved. Listed in Annex A are details of the different types of records generated by business units and the appropriate location to send them.

Retrieval of Records from MOD Archives

8.19. If there is a need to consult records which have been submitted to MOD Archives, originating business units can request their temporary return by contacting the relevant MOD Archive. In the case of records held in the MOD Sensitive Archives, requisitions should be sent directly to the MOD Sensitive Archive (See Annex A below). For records held at the MOD Main Archive an Asset Request Form should be forwarded to TNT.

8.20. Closed records recovered from the MOD Archives must not be added to or altered in any way and must be returned to the MOD Archives as soon as they are no longer required.

8.21. Guidance for using the MOD Archives can be found at Annexes B and C.

Sending Unregistered Records to MOD Archives

8.22. Unregistered records (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 for permanent preservation. Where they merit such consideration they should be forwarded to the appropriate MOD Archives as outlined below.

8.23. Unregistered 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 protective marking of the enclosed material, the year of its origin and the reason that its permanent preservation is being recommended must also be indicated.

Chapter 8 - Annex A

Where to send Records

Originator	Type of Record	Send to:
All	TOP SECRET and Codeword and files containing Atomic and Nuclear records. Further guidance can be found at Chapter 8, ANNEX A.	MOD Sensitive Archives 1st Floor, Building 2/003 Gloucester Road HM Naval Base Portsmouth PO1 3NH 9380 25252
All	Registered files (other than TOP SECRET and Codeword and files containing Atomic and Nuclear records). Further guidance can be found at to Chapter 8, ANNEX B.	TNT Archive Services Tetron Point William Nadin Way Swadlincote Derbyshire, DE11 0BB Tel: 0845 601 0610 Fax: 01827 312515 pangovarchive@tnt.co.uk
All	Service personnel records.	Refer to single-Service guidance
All	Civilian personnel records.	TNT Archive Services Tetron Point William Nadin Way Swadlincote Derbyshire, DE11 0BB Tel: 0845 601 0610 Fax: 01827 312515 pangovarchive@tnt.co.uk
Certain Air Force Department Files (See Chapter 7, Paragraph 7.33)	Other Air Force Department files, including TOP SECRET, Codeword and Atomic.	AHB1 (RAF) Building 824 RAF Northolt West End Road Ruislip, Middlesex HA4 6NG Tel: 95233 8160 Tel: 0208 845 2300 x 8160
All	All other records.	TNT Archive Services Tetron Point William Nadin Way Swadlincote Derbyshire, DE11 0BB Tel: 0845 601 0610 Fax: 01827 312515 pangovarchive@tnt.co.uk

Chapter 8 - Annex B

Forwarding Material to the MOD Sensitive Archives

General Guidance

8A.1. Business units should telephone or fax the MOD Sensitive Archives before dispatching more than 2 sacks of files, or other records for example books or ledgers, advising 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))**.

8A.2. Business units must keep a record of **ALL** material sent to the archive including the date of dispatch.

Registered Files

8A.3. Each file must contain a completed Registered File Disposal Form (MOD Form 262F) showing the disposal recommendation and full business unit address (at Part 3). Bundles of files should be clearly labelled and strapped or tied together.

8A.4. A MOD Form 24 (Receipt) containing the full business unit address and contact telephone number must accompany each individual sack. If the business unit is moving to a new address or being renamed, then the revised details should be included with the receipt.

8A.5. Remember that only TOP SECRET material and material requiring special handling is to be sent to the MOD Sensitive Archives. All other material should be sent to the MOD Main Archives at Swadlincote.

Unregistered Records

8A.6. Material not in registered files must be accompanied by a duplicate list of contents containing the business unit name, address and telephone number. One copy will be retained at by the MOD Sensitive Archives and the other returned as a receipt.

The address of the MOD Sensitive Archives is:

1st Floor, Building 2/003
Gloucester Road
HM Naval Base
Portsmouth
PO1 3NH

Chapter 8 - Annex C

Guidance on using the MOD Main Archives

General Information

8C.1. The following procedures should be complied with when either depositing or withdrawing files from the MOD Main Archive at Swadlincote. General guidance is shown below but for full details please refer to the TNT Archive Services Guide that can be found on the Defence Intranet.

Records and Receipts

8C.2. For all registered files, material that is not in a registered file, or bundles of material the following procedures apply:

8C.2.1. TNT Archive Services new business forms **MUST** be used and the collation codes used to identify the originating organisation and the record type being submitted to the Archive. A copy should be sent with the records which will be returned by TNT to acknowledge receipt.

8C.2.2. A record must be maintained of everything sent to the archives, including the date of despatch. TNT Archive Services cannot provide a retrospective list of material sent. An additional copy of the TNT Archive Services new business form would meet this requirement.

8C.2.3. A MOD Form 24 for each SECRET document, file, bundle, or sack (as appropriate) must be sent with full business unit address and contact telephone number written/stamped on back. If the business unit is moving or being re-named, put the revised details on the receipt.

8C.2.4. MOD Form 24 must only be sent for items protectively marked as SECRET.

8C.2.5. MOD Form 24 must be retained for 30 years.

8C.2.6. TOP SECRET material or material requiring special handling, **MUST NOT** be sent to TNT Archive Services – This material **MUST** be sent to the MOD Sensitive Archive in accordance with Chapter 8 Annex B.

Registered Files

8C.3. The following instructions for registered files apply in addition to those shown in paragraph 8A.3 above:

8C.3.1. The documents **MUST** be in Registered File covers – not Temporary Enclosure Jackets, branch folders, or bundles of loose papers, etc.

8C.3.2. Each file **MUST** contain a completed MOD Form 262F showing: full file title and reference (for example 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 number; and a signature of the reviewing officer of the correct grade (Band C2/Service equivalent or above).

8C.3.3. A copy of the MOD Form 262F **MUST** be retained for the business unit record of all files archived at the MOD Main Archives.

8C.3.4. Large/bulky files are to be strapped; otherwise they may split/fall apart when opened and papers will be lost.

8C.3.5. File titles/Numbers on covers are to be clearly legible.

8C.3.6. Empty file covers containing no other papers should not be sent to the MOD Main Archives.

8C.3.7. Records which are due to be destroyed imminently should not be sent to the MOD Main Archive.

8C.4. Files lacking details at paragraphs 8C.3.1 and 8C.3.2 above will NOT be accepted by TNT and will be returned to sender.

Unregistered Records

8C.5. Unregistered 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.

8C.6. This type of material must NOT be mixed with registered files and the correct collation identified on the new business form. For information about collations see Defence Intranet. It is stored in a different section of the archive.

Bundles

8C.7. Bundles of files or other material must be:

8C.7.1. Clearly labelled; and

8C.7.2. Strapped together with 2 copies of a list of contents.

CHAPTER 9

Joint Operational Records Keeping

Introduction

9.1. The Key Operational Record (OR) is intended to provide a factual summary of important events and decisions in the course of an Operation involving Units and must 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 Commanding Officers and soldiers against false or malicious allegations; provide the necessary detail if required in legal cases; and is the de facto authoritative history of the operational events in theatre.

9.2. The OR is a subset of all the information created in Theatre, collates all the important documents and information produced as part of the normal routine staff process during operations, is a record which fulfils departmental needs and is selected for permanent preservation.

9.3. The setting of policy, procedures and processes for the capture and management of Single Service Key Operational Records is the responsibility of the Single Service Historical Branches. The Single Service Key Operational Records Keeping (ORK) policies can be found in:

- BR 9461 - Operational and Historical Record Keeping Policy;
- LFSO1120 – Operational Record Keeping (ORK); and
- Queen’s Regulations, Paragraphs 2137 and 2138 - Booklet AP3040: “Operations Record Book” – Form 540.

9.4. For further information regarding Single Service Key Operational Records please contact:

- Navy Historical Branch for the Royal Navy, Royal Fleet Auxiliary (RFA) and Royal Marines;
- Corporate Memory Analysis for the Army, PJHQ and any other Joint Headquarters or Units; and
- Air Historical Branch for the Royal Air Force.

Joint Formations

9.5. Joint Formations, which are defined as deployed headquarters of two stars and above consisting of at least two Services, must liaise with Corporate Memory Analysis (see paragraph 9.19 below), who in their coordinating role with the other Single Service Historical Branches, will arrange the method for the capture of the Joint Formation’s OR.

9.6. Whenever possible a Corporate Memory Analysis directed historian will accompany a deployed Joint Formation to either produce or advise on the production of the Joint Formation’s OR.

9.7. If it is not possible to deploy a historian, Corporate Memory Analysis will instruct how the record from Joint Formations should be captured on a case by case basis.

Joint Units

9.8. The remainder of this chapter applies to deployed Joint Units where a Joint Unit is defined as a unit below two stars in which elements of at least two Services participate, which has been formed for a specific operation. Standing Joint Units must continue with their existing ORK arrangements.

9.9. At the start of an operation (including operations in the UK), PJHQ or whichever Single Service Headquarters is responsible for the Joint Force Generation, must consult Corporate Memory Analysis who will decide with the other Historical Branches where the Joint Unit is to submit its OR and which Single Service Operational Record Keeping process it is to comply with.

Responsibilities

9.10. It is the responsibility of the Commanding Officer for the Joint Unit to ensure that the Joint OR is maintained and sent to the nominated receiving Historical Branch at the end of each calendar month. Apart from exceptional circumstances, the Commanding Officer is to sign the Joint OR produced.

9.11. Responsibility for the Joint OR rests with the Commanding Officer. The task of producing the Joint OR, however, may be delegated by the Commanding Officer to the Second in Command in the unit as long as they are of appropriate rank and competence.

9.12. Where a Joint Unit is included in the Joint OR of a higher level unit then it is the responsibility of the unit Commanding Officer to ensure that their force element is fully represented in the higher level OR.

Unit Contact

9.13. When the Joint OR is opened the officer responsible for its compilation must contact the nominated receiving Historical Branch (see paragraph 9.19 below) and provide the following details: Joint Unit Title, Name, Appointment, Telephone Number and E-mail Address.

9.14. This initial contact will allow questions to be asked on any unfamiliar aspect of the ORK process and will ensure that the correct ORK forms are in use. As the operation progresses, continued liaison between the nominated Historical Branch and the officer responsible should ensure the easy resolution of any problems in the compilation or dispatch of the Joint OR.

9.15. The requirements for the Joint OR are no different when British Forces are serving under foreign military command, such as NATO or the UN. The same materials must be included covering the same subjects and organised in the same logical manner, and the Joint OR must be returned to the nominated receiving Historical Branch as outlined in this policy. This requirement remains regardless of whether operational records are to be provided to the foreign military command. If necessary, duplicate copies of the Joint OR should be made for this purpose.

9.16. Where foreign units are serving under British military command, the British units or formations under which they serve should include their (the non-UK units') reports and returns in the OR as if they were a British Unit or Sub-unit. Foreign units in this position are not otherwise required to provide an OR.

Submission

9.17. Joint ORs must be submitted at the end of each calendar month to the nominated receiving Historical Branch who will be the custodian of the Joint OR and retains Joint ORs once completed. The OR must be received by the nominated receiving Historical Branch by the end of the following month.

9.18. Monthly returns allow the nominated receiving Historical Branch to answer near real-time questions on an operation and assist with the early resolution of problems with the Joint OR.

9.19. Monthly Joint OR submissions must be sent to the nominated Historical Branch which will be one of:

Corporate Memory Analysis
Chief Information Officer
Level 3, Zone G
Ministry of Defence, Main Building
C/O TNT
Pages Walk, Bermondsey
London, SE1 4SB
Military Network: 9621 80931 / 89329 / 89298
Telephone: 0207 21 80931 / 89329 / 89298
Facsimile: 9621 70331 or 0207 807 0331

Naval Historical Branch
The Curator
No. 24 Store
PP20,
HMNB Portsmouth
PO1 3LU
Military Network: 9380 24893
Telephone: 023 9272 4893

Air Historical Branch
Building 824
RAF Northolt
West End Road
Ruislip, Middlesex
HA4 6NG
Military Network: 95233 8162
Telephone: 0208 833 8162
Facsimile: 95233 8075

Monitoring Process

9.20. The nominated receiving Historical Branch must maintain a monthly record of returns from Joint Units. At the beginning of the first week of every calendar month, a list of Joint Units which are overdue with the submission of their Joint OR or whose Joint OR is inadequate, will be sent to the operations branch of the Headquarters responsible for the operation on which the Joint Unit is deployed, which in turn will pass it down the chain of command instructing that the Joint OR be completed. Failure to comply after 3 months will result in the nominated Historical Branch issuing a letter containing a “statement of non-compliance” to the Commanding Officer of the Joint Unit.