Ministry of Defence

D3, Building 405

Corsham

Wiltshire SN13 9NR

United Kingdom

Reference:
FOI2017/02121

E-mail: ISS-SecretariatGpMbx@mod.uk

30th March 2017

[redacted]

FREEDOM OF INFORMATION REQUEST

Thank you for your e-mail of 9 February 2017 requesting the following information:

"- Do you make use of any Instant Messaging clients/systems, such as group clients like Yammer, Slack, Whatsapp groups, Facebook or Twitter message groups or user-to-user Google Chat type services etc?

If yes, please provide a list with details of each with its use, membership (to the extent it is disclosable, such as categories) and service as well as any 'service tier' information held and cost where applicable. This would include personal chat groups used in a way that would bring them into scope of the Freedom of Information Act.

The following questions are conditional on the answer being yes:

- For each of the above, are you the data controller? Is it a shared service (e.g. use of https://ukgovernmentdigital.slack.com/) or your own system?

- Where one of the above is a Slack or similar 'cloud' chatroom with a unique URL, please provide this link.

- Where one of the above has a specific membership criteria, please provide this.

- For each of the above, how long is information retained for and in what form?

- For each of the above, please provide copies of any relevant policies or procedures regarding records management, retention or FOI/EIR/DPA compliance."

I am treating your correspondence as a request for information under the Freedom of Information Act 2000 (FOIA). A search for the information has been conducted and I can confirm we do hold information within the scope of your request. However, some of the information in scope falls under the following qualified exemption: Section 26 (Defence) and is therefore withheld.

Microsoft Messenger and Skype for Business are official applications provided by MOD to staff for internal communications only within the MOD; information exchanged on Microsoft Communicator is not retained. Microsoft Communicator is available to users of Defence Infrastructure and Information (Dii) as part of Office 2010, and Skype for Business is available for use by MODNet users as part of Office 365. MOD is the data controller for these services.

This is our formal provision, smaller formations may use other products where there is a business need and taking security considerations into account.

The policy relating to use of IT systems is contained within Joint Services Publication 441: Managing Information in Defence. A redacted copy of JSP 441 is enclosed.

Information about the potential use of other instant messaging clients/systems is withheld under Section 26 of the FOIA.

Section 26(1)(a) of the Act provides that information is exempt if its disclosure would, or would be likely to prejudice the defence of the British Isles or of any colony and Section 26(1)(b) provides that information is exempt if it's disclosure would, or would be likely to prejudice that capability, effectiveness or security of any relevant forces. Release information in scope of your request would increase the risk of a successful attack on MOD IT systems, with the potential risk of further information being consequently released which could further compromise the defence of the UK and potentially other forces the UK may work or share information with.

The level of harm involved in the release of this information is judged to be at the higher level of 'would' prejudice.

This exemption is qualified and therefore it is subject to a public interest test (PIT); the public interest arguments relating to the use of this exemption have been considered and the balance of public interest lies heavily in favour of maintaining the use of this exemption, as to release information in scope of your request would increase the risk of further information being consequently released which could further compromise the defence of the UK and potentially other forces the UK may work or share information with.

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

If you remain dissatisfied following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not investigate your case until the MOD internal

review process has been completed. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website www.ico.org.uk

Yours sincerely,

Information Systems and Services (ISS) Secretariat

Ministry of Defence

JSP 441

Managing Information in Defence

Part 1: Directive

JSP 441 Part 1, v1 1, Jan 2017)

Foreword

Information is the lifeblood of Defence and acts as a 'force multiplier', enhancing our effectiveness. This applies in military operations and in all that we do to prepare for, and support, those operations, as well as in our role as a Department of State. The better we use the information that is available (or potentially available) to us, the more effective we will be – individually and as an organisation.

Information comes in many forms:

- it may be recorded, perhaps on paper, or in portable electronic devices, or in computer centres;
- it may be unrecorded, such as knowledge in our heads;
- it may be current, recent, or historic;
- it may be static (like a reference document) or dynamic (like an operational picture);
- it may be structured data (eg logistics, pay, measurements) optimised for machine processing, or unstructured (typically text, graphics, audio and video) usually requiring human interpretation.

All Defence Information should be:

- legally held and used;
- correctly labelled and stored;
- readily available in a helpful format to those who should have access to it;
- securely protected from those who should not have access to it;
- preserved for an appropriate period of time.

As CDIO I sponsor two major JSPs, this JSP 441 for Information, and also JSP 604 on Information and Communications Technology (ICT) in Defence. This reflects my dual role as Defence Authority for Information, and as the lead for provision of ICT. It is important that we distinguish between the Information itself, and the ICT that we use to capture, process, store, find, communicate and present that Information.

The success of Defence depends on how we manage and use our information. JSP 441 is designed to enable us to do this effectively.

Mike Stone

Chief Digital and Information Officer

Defence Authority for Information

December 2015

Preface

How to use this JSP

This JSP contains Policy, Rules and Guidance on Managing Information in Defence.

Part 1 provides a summary of our aims in the way we manage and use information, and what must be done in order to meet those aims. It also contains a set of rules that must be followed to ensure that we manage data effectively and maintain good records – this is to ensure that we use corporate reference data appropriately, and that we never lose or destroy any of our most important material.

Part 2 contains guidance, in the form of topic-based guides. Some of these are intended for us all; some are for particular specialist tasks. Part 2 begins with an index of these guides, and this index shows whether the topic is general or specialist, and the general category.

The JSP is designed to be easily read and understood by all staff. Everyone handles information, so it is important that we understand the key principles around organising, sharing, protecting and preserving information – all this can be found in Part 1. We can then find more detail in Part 2.

This JSP supersedes the existing JSP 329 (Information Coherence for Defence), JSP 441 (Defence Records Management Policy and Procedures), JSP 717 (MOD Metadata Standard), and JSP 747 (MOD Information Policy). As part of Defence's overall aim to reduce the volume of published policy and guidance, some of the former material is no longer included.

Training

The Defence Academy provides training for staff in professional Information roles. More details can be found here, and at the DefAc Course Prospectus on Information Capability. This training includes classroom courses for Senior Information Officers, for Information Managers, for Information Support Officers, and for Information Support Assistants. There are also on-line courses in the Defence Learning Environment, including the Information Management Passport.

Feedback

Comments, queries and feedback are welcome, via this email address, or via the Information Portal on the Defence Intranet (accessible through the 'Policy & Guidance' tab, and then 'Defence Authorities').

Contents

1 Defence Information Policy

Background

1. Information is the lifeblood of Defence, and it comes in many forms – it may for example be on paper, in portable electronic devices, in computer centres, or in our heads. Typically we use the terms:

- 'Data' to describe numbers, words or images held in (or designed to be read by) a computer or other processing device;
- 'Knowledge' (or sometimes 'Tacit Knowledge') to describe that which is known by people in their heads, rather than what is in recorded form.

2. 'Information' can cover both Data and Knowledge, as well as that which is held in recorded form and can be read and understood by a person. The meaning of the word 'Information' is usually determined by its context. So when we are talking about 'labelling' or 'storing' information, we assume that information is in recorded form – if we are talking about 'communicating' (without saying what the medium of communication is), then it could equally well be communication of knowledge.

3. How well we use information depends on how readily we can find it, how quickly and helpfully it is presented, and the skills we have. Defence is a team game – each one of us relies on information created, published, and communicated by others, and we depend too on the technology we have to help us. It is therefore essential to manage our information carefully in order to ensure that individually and organisationally we can exploit it effectively.

4. Achieving perfection in managing information is beyond any large organisation; we must therefore concentrate on information that is likely to be of value.

5. We must comply with the law, and particularly the four main Acts covering the way that we manage and use information in Defence:

- The Official Secrets Act
- The Public Records Act
- The Data Protection Act
- The Freedom of Information Act

6. Brief summaries of the Acts, and how they relate to our work, are at this link.

7. We must also comply with overall Government policy and guidance, in particular:

- Security Policy Framework
- Code of Practice on the management of records
- Information Commissioner's Guidance

Defence Information Policy (in a few lines)

8. The MOD's policy is that information should be:

- Legally held and used;
- Correctly labelled and stored;
- Readily available in a helpful format to those who should have access to it;
- Securely protected from those who should not have access to it;
- Preserved for an appropriate period of time.

Requirements for success

9. For this policy to succeed, we need to develop and sustain the following five components:

- Good doctrine and guidance which must be easy to find, easy to understand, and easy to follow;
- Appropriate skills in handling information, and in using the associated technology, supported by high quality readily accessible training;
- Effective governance, to help people manage and use information well;
- Modern, fast, flexible and reliable ICT that is easy to use, and which supports people in managing and exploiting information;
- Strong leadership at every level to set high standards and inspire effective teamwork.

2 Our Responsibilities

Corporate and Personal Responsibilities

10. The next headings cover:

- What the MOD collectively will aim to do;
- What Information Specialists must do – this is of interest mainly to people who have the word Information in their job title (or of course related terms, including Data and Knowledge);
- What ICT Project Managers must do – this is to help ICT Project Managers deliver systems that will help the MOD, and all of us using those systems, do the right things with information;
- What Leaders and Managers must do – there is extra responsibility on you if you are in a leadership role;
- What everyone in Defence must do – this applies to us all.

What the MOD collectively will do

11. To provide the right overall environment for successful management and use of information, the MOD will:

- appoint a Chief Information Officer (CIO), to be the Defence Authority for the way in which information is handled. Currently this role also includes that of Digital Leader for Defence, and is known as Chief Digital and Information Officer (CDIO);
- appoint a Senior Information Risk Owner (SIRO);
- require that each TLB and other authority defined in the current version of the Defence Operating Model appoint a senior officer responsible for the way in which information is handled in that Command;
- delegate authority for managing information effectively through the Defence Chain of Command;
- require that Data Owners and Data Stewards are appointed to be accountable for the quality of the relevant data and Management Information (MI);
- require all data in Defence to have an accountable, responsible owner, the Defence Data Authority, identified;
- require that each unit has an appropriate information governance structure in place, as determined by the local Command;
- maintain centres of expertise in specialist areas, in particular for compliance with information law, and with analysis of historical information;
- publish guidance, support and tools designed to help units and each person in Defence manage and use information effectively;
- make available appropriate training and support and for everyone in Defence, whether generalists or information specialists;
- aim to provide modern, fast, flexible and reliable ICT that is easy to use, and which complies with Cabinet Office standards for security of the information it stores or processes;
- aim to ensure that all environments where information is stored and

processed (primarily but not exclusively ICT) support the requirements to share, protect and preserve information effectively;

- provide direction and guidance to ICT projects on how information should be structured and exchanged;
- provide policy, strategy and standards for MI and data;
- publish authoritative reference data and the Defence terminology, to be used in MOD systems;
- publish a standards hierarchy, with the preference to use formal International Standards where they exist;
- follow Government Metadata standards;
- identify and understand information risks, making sure they are expressed clearly and concisely, carefully managed, and appropriately presented to those responsible;
- continuously improve information handling, through better processes, better skills, and better technology;
- encourage the gaining and responsible sharing of knowledge among its staff through training, education, guidance, experience, leadership, processes and culture;
- contribute to, and support, pan-Government information agendas;
- hold everyone in Defence responsible and accountable for the information they handle and set high expectations of conduct.

12. For legal compliance, the MOD will:

- manage and use information through life in accordance with the law, with Government policies, and in the best interests of Defence;
- follow the rules and guidance in the current editions of;
  - HMG Security Policy Framework;
  - Lord Chancellor's Code of Practice on the management of records;
  - Information Commissioner's Guidance;
- publish and publicise an Acceptable Use Policy.

13. To enable useful information to be correctly labelled and stored, MOD will aim to:

- process and store information in known and controlled environments where it can be properly protected, readily retrieved, and easily shared;
- provide (directly or indirectly) such processing and storage environments, along with rules and guidance so that they can be effectively used;
- adopt or provide standards for labelling and formatting of information, appropriate to the type of information and the storage environment concerned.

14. To make information readily available to those who should have access to it, the MOD will:

- promote a culture of responsible information sharing, whether that information is in recorded form, or what people know;
- appoint a Head of Profession for Knowledge and Information Management,

to provide a voice, and a sounding board, for good practice;

- embed ways of working where people store all significant recorded information in a sensibly named, and appropriately protected, shared area;
- communicate information effectively, making it easy for people to choose the appropriate channel;
- have adequate skills, processes and technology to maintain Business Continuity in response to disruption;
- through appropriate processes and technology, ensure people with disabilities do not face unnecessary barriers in access to, and use of, information;
- collaborate and share information with external bodies (such as Allied Nations, Treaty Organisations, Other Government Departments, and Industry partners), respecting the information belonging to others;
- provide information to people outside Defence with a legitimate right to it.

15. To protect information securely from those who should not have access to it, the MOD will:

- ensure that people accessing the environments where information is processed and stored are appropriately security cleared and authenticated;
- ensure that devices accessing these environments are also authenticated, and are appropriately secured against use by unauthorised people;
- ensure that data at rest and in transit is appropriately secured;
- establish systems and processes for protecting networks;
- establish a system whereby all Defence staff can report security concerns direct to specialist staff;
- publish Security Operating Procedures (SyOPs) for all MOD ICT services.

16. To preserve information for an appropriate period of time, the MOD will:

- appoint a Departmental Record Officer, responsible for ensuring that the correct information is retained;
- ensure that information is not lost due to failures in Digital Continuity (e.g. technology obsolescence or media degradation);
- ensure that information is not lost to the MOD because of failures to select or manage service suppliers adequately;
- promote good practice in the acquisition and transfer of knowledge as jobs and people change;
- promote good practice in the safe disposal of information which has no residual value;
- ensure that important information created or acquired in operational theatres, or in other places where it would be difficult to manage it safely over a long term, is recovered into more benign information management environments for retention;
- ensure that information from units that are closing or changing substantially is cleansed and passed on to a successor, or to a higher authority;
- ensure that information likely to merit long term preservation, and possible accession to The National Archives, is managed with special care.

What Information Specialists must do

17. Many people in Defence have specialist information roles, either as primary or secondary tasks. They may be working in organisations whose primary responsibility is some aspect of Information Management, or they may be a local information specialist in mainstream Defence units. If you are in such a role, then you should:

- understand the main aspects of information legislation, HMG policy and guidance, and MOD policy and guidance;
- stay current with updates from Government authorities (in particular Cabinet Office, the Information Commissioner, The National Archives and GetSafeOnline), MOD CIO, and Information staff within your Chain of Command;
- support others in understanding the essence of good information management and use, and in complying with the policy;
- identify information risks to your Chain of Command;
- monitor activity in the management of information in your area, identify potential improvement whether in policy, guidance or practice, and inform the responsible people;
- set a good example in all aspects of managing and using information.

What ICT project managers must do

18. Effective sharing of information across Defence requires the use of common structures, terminology and information exchange protocols. You should:

- understand the Defence Terminology, MOD's Authoritative Reference Data, Data Exchange Policy and Standards Hierarchy, and ensure these are used appropriately;
- consider any wider implications, deployability and benefits of the applications, the service, and the information processed, to add value for Defence.

What leaders and managers must do

19. Whatever environment you work in, your success will always depend on you and your team being effective in acquiring, understanding, sharing, protecting, retaining and using relevant information. How you do that will depend on your role and your style, but you should:

- ensure that everyone in your team understands the importance of handling information effectively, does the relevant training and follows good practice;
- ensure that everyone in your team understands the value of timely and accurate information, and appreciates how to use it, especially to support effective decision-making;
- ensure that your team has, or quickly gets, the relevant information needed to do their job effectively;
- make appropriate arrangements for sharing and transferring knowledge when jobs change, when people change, and to provide adequate cover for absences and gaps;
- support and encourage your local Information Specialists, and of course, set an excellent example!

What everyone in Defence must do

20. We all handle Defence information, whether on computers, on paper, or through the spoken word. We need to do it well, keeping within the law and obeying our Service Code of Conduct. As part of our job, we must share information responsibly with those who need that access. We must also ensure that it is not disclosed to unauthorised people – that applies to Defence information (especially if it is protectively marked in some way) and to personal information about other people. If the information is likely to be of value, then it needs to be recorded in the right way, in the right place.

21. You should:

- understand and abide by your legal obligations under the Official Secrets Act, the Data Protection Act, and the Freedom of Information Act;
- understand and handle information in line with the Government Security Classification rules;
- understand the basic principles of good information management as published by the MOD CDIO or TLBs;
- know where to find published guidance, and how to use it;
- follow good practice in labelling, storing, sharing, protecting and preserving information;
- when appropriate, make a written record of the knowledge and expertise that you bring to your job, to make it easier or more reliable to share with others, or to ensure that actions or decisions made at the time can be understood in the future;
- prepare and store records correctly, as detailed in Section 3 (Records Management Rules);
- understand and follow the MOD's Acceptable Use Policy which applies when using any MOD ICT equipment;
- stay in date with MOD mandated information training;
- understand how to use the ICT provided by the MOD for your job;
- follow the Security Operating Procedures (SyOPs) for any MOD ICT that you use;
- report any risks and areas of concern;
- help colleagues to work effectively with information;
- remember the importance of good Personal Security, Information Security, Operational Security, and Communications Security at all times, on duty or off, whether using the MOD's ICT or your own, or no ICT at all;
- know your local Information staff, and when in doubt, ask!

Rules for Managing Data

22. High quality information is required to support the delivery of Defence capability, generate reliable management information, and inform key decisions in both the operational and business space. Fundamental to this is underpinning data that is consistent, accurate, relevant, timely and trustworthy. Typically we use the term 'data' to describe numbers, words or images held in (or designed to be read by) a computer or other processing device. All data can be structured, unstructured or partially/semi structured as detailed in the Foreword. Big Data is simply very large datasets and is often the subject of complex analytical work to spot trends and patterns. This data can be invaluable in both the business and operational space and may contain large quantities of sensitive information. The process of working with large volumes of data that can be exploited in various forms is commonly referred to as data science.

23. To achieve the standards required we need to meet a number of policy requirements that Defence must implement so that it can meet its legal obligations and fully exploit its data. Key to this are the Defence Data Authorities (DDAs), which are charged with ensuring that data in their area of responsibility is:

- securely protected while remaining fully searchable and accessible to those with an authorised need to see and use it;
- well managed and governed from point of creation to point of archive or destruction;
- authoritative – created once and used many times;
- in a recognised standard format to enable it to be fully exploitable and interoperable with other systems both existing and foreseeable;
- correctly labelled with consistent metadata (data that accurately describes it);
- of sufficient quality to meet Defence's requirements;
- fully risk assessed ie risks to the security, quality and completeness of the data are identified, documented and mitigated.

24. Whilst the ultimate responsibility for the above is on the DDAs, everyone in Defence carries an equal responsibility to meet those requirements. Business areas can expand on these rules to meet their requirements and therefore produce data management policies that are tailored to their specific needs, drawing out and expanding on the top level requirements outlined above and in the more specific rules that follow.

25. DDAs must implement the data management rules below for their area of responsibility. These rules will be expanded to accommodate the new requirements following delivery of the Defence Data Management Reference Architecture (DDMRA) and the Defence Enterprise Data Model (DEDM), Personnel element both of which are expected March 2017.

<u>Governance</u>

- Establish formal governance regimes.
- Keep accurate records of where and how the data is used that clearly shows dependencies – this will usually be in the form of a data model.
- Establish and implement through life data management plans.

- Report to the Chief Digital Information Officer (CDIO) on the progress of data management initiatives and activities within the timeframes specified by CDIO's designated agent.
- Use Defence data definitions from the MOD approved repository, currently the Reference Data Manager (RDM), or add their definitions to it if nothing suitable exists in the RDM.

Availability

- Defence data must be easily and quickly available and retrievable to all who have an approved use for that data and protected from those who do not.
- Data stewards are to ensure that the relevant data to be shared in their system(s) is transformed into one of the mandated standard data formats[1].
- Authoritative data shall not be reused without authorisation from the relevant Data Steward.
- Where the data to be shared has not been identified as authoritative, the DDA must formally authorise its release.

Quality

Data must be:

- Accurate - reflecting the real world objects it represents. No additional interpretation or cleansing should be required.
- Complete – the full dataset required to meet the business need must be captured and kept up to date within the agreed parameters.
- Relevant – applicable and helpful for the task at hand.
- Valid - data values must conform to the attributes associated with the data element.
- Reported - DDAs are to implement data quality reporting regimes in accordance with the requirements of the Defence Data Management Balanced Scorecard.

Security

- Defence data is to be managed in accordance with UK data protection legislation and Government data security policy (as applicable).
- All data and management information systems must comply with Defence Security Policy (JSP440).
- Data security reporting must be implemented in accordance with the requirements of the Defence Data Management Balanced Scorecard.

Labelling and Descriptions

- The MOD Taxonomy and Thesaurus are the MOD approved source of terminology and must be used for MOD resources.
- Content Management Systems must enable users to allocate terminology from the MOD Taxonomy and Thesaurus.
- Independent glossaries should not be created - the MOD Glossary is the official source of definitions and acronyms and must be used.

[1] The Management Information team, ISS Des-CMI-DAMI-KIM, can provide guidance on these.

Identifiers

- All entities of a particular type must be individually referenced or catalogued electronically/uniquely identified using a commonly implemented scheme.
- The system must not allow re-use of an identifier and should be capable of quickly and easily interfacing with existing identifiers and scale to meet any foreseeable requirement.

The following identifiers are widely used across Defence:

- Unit Identity Number (UIN) - this must be issued and managed through correct completion of Form 942 (F942) (see link). Instructions and rules relating to its format can be found through the F942 intranet page.
- Person Unique Identifier (PUID) - all new applications that utilise personnel data must have the ability to utilise the MOD approved personal identifier, currently the PUID.
- Electronic Unit Name (EUN) - refers to a unit as determined by the owning TLB organisation within specified format constraints. These are published and managed by Defence Business Services (DBS) (see link). EUN will be replaced by Business Owner in MODNet but it is expected that broadly similar formatting constraints, as detailed in Part 2 of this policy, will apply to maintain brevity and coherence across Defence.
- Electronic Role Names (ERN) - specific role names based upon the EUNs, and must utilise MOD approved abbreviations. Users can request new and changes to the ERN Abbreviation List through DBS. In MODNet these will appear alongside the user's name in brackets so brevity and consistency is essential. Format constraints are listed in Part 2 of this policy.

Rules for Managing Records

Overview of Records Management

26. This section of the JSP on Managing Information in Defence explains what needs to be done, corporately and individually, to ensure that there is an accurate and comprehensive record of the work of Defence. It is included here because it contains specific rules that we all need to be aware of and follow, although much of the implementation will be carried out by Information specialists.

27. The following topics are covered:

- Overview;
- Capturing Information and Declaring Records;
- Managing Records Created On Operations;
- Classifying Records, and Maintaining File Plans and Retention Schedules;
- Storing Records;
- Disposing of Records;
- Summary of Records Management Rules;
- List of document types which must be preserved as records.

28. 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:

- are present;
- can be accessed by those entitled;
- can be understood;
- can be trusted as being authentic;
- can be disposed of when no longer required.

29. 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.

30. Each of us working in Defence must ensure that we maintain accurate records, storing it correctly in accordance with the rules here, and as required by our unit.

Capturing Information and Declaring Records

31. Effective records management begins by ensuring that we capture the right information, label it correctly, and store it in the appropriate shared area with the necessary access permissions. Declaring the document (using the word ‘document’ in a broad sense) as a record provides assurance that it will be subject to an appropriate retention schedule, and protected against amendment or premature deletion.

32. The way that this is done will vary with the technology being used, the term ‘declaration’ usually indicating that this is a two-phase process in an electronic environment. The same principles apply, even though technologies will differ.

33. Important material must be saved as records, in particular:

- any material that would be regarded as a significant Historical Record, which will include the documents summarised in the last paragraph of this section;
- records retained for Legal or Audit Purposes, including legal, finance and accounting records, contracts and agreements (noting that these may need to be retained in hard copy as well);
- material from operations (see section below).

34. For other material, some judgement will be necessary on what information needs to be preserved longer term. As a general principle, we should declare as records that material which has corporate value (short or long term), including:

- documents which contribute to a discussion or a decision, such as policy documents, reports, reviews, guides, as well as any correspondence sent externally;
- documents produced regularly as part of an administrative or operational process, such as minutes, meeting papers, data returns, reports, Memoranda of Understanding, and audits.

35. In general, ephemeral documents, rough drafts, spare copies, etc. need not be declared as records if they are not of any lasting significance. Such documents should be destroyed when no longer needed.

36. 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.

37. It is important that people across Defence understand what records should be kept. As the specific types of information will be different for each business unit, then each unit must ensure that its staff know what is to be kept, where, and how.

Managing Records Created On Operations

38. Units and Formations must maintain a comprehensive record of their activities whilst deployed on operations (including Operations in the UK). This applies equally to the period when training or otherwise preparing for operations.

39. All such records must be correctly labelled and stored, and operational information created in overseas theatres must be returned to UK. These records must then be retained within the MOD for a period of at least 15 years, and until specific approval by the Chief Digital and Information Officer to dispose of it, or until transfer to Defence Business Services (DBS) to review. Standard governance will apply: the creating unit (or a successor unit, or the higher authority) will be responsible for the records.

40. A subset of these records created on Operations will be defined as Key Operational Records. These are high value records, whose content and format are specified by Joint Unit or Single Service Key Operational Record Keeping policies. Once transferred to the relevant Historical Branch, that Branch becomes responsible for the management and resolution of information requests.

41. These Key Operational Records provide a body of information that can be used by the Historical Branches for operational analysis, development of operational capability, and lessons identification. They also form the basis of the record for any legal or disciplinary activity, although of course any records may be relevant. Successive judicial inquiries have stressed the importance of effective record keeping. Good records are vital in defending MOD, Units, Commanding Officers and individuals against unwarranted claims.

42. Key Operational Records also form the records of operations that the MOD will transfer to The National Archives for permanent preservation.

Classifying Records, and Maintaining File Plans and Retention Schedules

43. Classification is the process of grouping similar information within a business unit together. In paper systems, this is achieved through placing documents on particular topics in a specific file, and having a file numbering system that reflects the general type of file. Similar processes are necessary in electronic systems, as they facilitate description, search, browsing, access control, review and final disposal.

44. The classification scheme is generally known as a file plan. A well structured and maintained file plan makes it easier to:

- see where information should be correctly stored;
- obtain a continuous record of activity;
- retrieve all records relating to a particular function, topic or activity;
- achieve security and manage access;
- manage retention, review and disposal of records.

45. Metadata. Appropriate metadata needs to be associated with all folders in the file plan, whether these folders are paper or electronic systems. At a minimum the metadata should include: name/role of folder owner; keywords; retention schedule; and a description of intended content.

46. Closing Folders and Parts of Folders. To aid cross-departmental thematic review, and allow related records held on different systems (for example at different levels of security classification) 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. Files and folders should be closed altogether when it seems unlikely that new material will be added.

47. Retention schedules are an essential aspect for all records management systems. They ensure that records will be retained for a specific period, and are then eligible for review to determine appropriate disposal action for a particular folder (or further retention). Appropriate retention schedules must be applied to every folder and registered file in the file plan hierarchy.

Storing Records

48. It is essential that MOD records are stored in a way that they can be readily accessed in their original form and in the right context, appropriately secured, and preserved so that they remain accessible into the long term. The MOD must therefore provide appropriate storage environments, meeting the technical standards published by The National Archives, and managed through life.

49. In order to ensure that a record can be safely preserved, the following rules must be followed:

- Offline Storage. Electronic records are not to be maintained on off-line media (such as CDs). Such material should be transferred to a controlled storage environment as soon as practicable;

- Misfiled Records. If records have been misfiled, then they should be transferred to their proper location. An audit log is to be maintained 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. Unless there has been misfiling, records are not to be transferred (there may be technical migration

to another platform, but the folder structure must remain intact);

- Encryption. Records must be declared in unencrypted form (otherwise there is a high risk of loss);
- Digital Signatures. A digitally signed document may be declared as a record, but the content must be in unencrypted form (as above);
- .pst files. This is a file type used within Microsoft Outlook, mainly to save emails to personal offline environments. These .pst files are not to be declared as records (very high risk of loss);
- Self Modifying Fields. Some documents are created with fields that automatically update to reflect current date/time. This is clearly not good for records, so self-modifying fields are to be made permanent prior to declaration;
- Reference Material. Any information referenced within a record should itself be accessible in the correct version and format. It may be necessary to file such material into the same folder as the record, although for external documents there may be copyright restrictions that prevent this (in which case a suitable note should be made).

Disposing of Records

50. Eventually all records must be disposed of – the questions are 'When?', and 'How?'.

51. A small proportion of the MOD's records will be sufficiently important to be retained permanently in The National Archives. Other records will be of long term value to the MOD, and need to be retained in the Department: this will include for example records related to military equipment that is still in service, as well as material related to Operations.

52. There are also limitations on destruction of any material related to certain operations or topics, even if the material looks of low value. The MOD will announce these by DIN. Currently (2015) there are bans on destruction of material related to:

- Operation Banner (Northern Ireland) (2014DIN03-022)
- Operations in Iraq (2013DIN03-009)
- Operations in Afghanistan (2013DIN03-009)
- The Independent Inquiry into Child Sexual Abuse (IICSA) (Goddard Inquiry) (2015DIN05-019).

53. Under Public Records legislation, any material that the MOD wishes to retain above a certain age (progressively reducing from 30 to 20 years between 2013 and 2023) must be approved by the Lord Chancellor, through a Lord Chancellor's Instrument (LCI). Also, under the Data Protection Act, personal data must not be kept for longer than necessary.

54. So there is a balance, and judgement is necessary. If there is doubt, specialist advice is to be sought from the unit's TLB.

55. There are some specific rules that must be followed:

- TOP SECRET Folders/Registered Files. Folders/registered files containing TOP SECRET and/or codeword material records must not be destroyed locally. Once no longer required for business purposes, all registered files containing TOP SECRET material are to be forwarded to the MOD Sensitive Archive, even if the Registered File Disposal Form (MOD Form 262F) recommends that the file should

be destroyed). Custodianship of electronic folders containing TOP SECRET material is to be transferred to the DBS KI Records Review team.

- Weeding of Folders. The weeding of ERMS folders or registered files or folders is prohibited. TNA requires the MOD to select complete files for permanent preservation rather than extracts from files, to ensure that preserved documents retain their original context.

- Metadata. When we destroy records, we need to retain evidence of that destruction for a minimum of 20 years. This should be done on MOD Form 262F for paper records, or an electronic equivalent.

Roles and Responsibilities

56. The Departmental Record Officer (DRO) is to fulfil the role as published by The National Archives (TNA), and in particular is responsible for:

- ensuring MOD information is managed from the point of creation until it is destroyed or transferred;

- selecting information for permanent preservation in accordance with TNA policy and guidance;

- transferring selected records to TNA.

57. Defence Business Services (DBS) is responsible to the DRO for:

- managing the MOD's archives, either directly or through a specialist supplier;

- reviewing records, selecting important records for transfer to TNA, and disposing of all material appropriately when no longer required.

58. 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.

59. Single Service Historical Branches are responsible for:

- administering the capture and subsequent management of Key Operational Records.

60. Developers of operationally deployable ICT systems are responsible for:

- implementing an archiving capability for the ICT system, approved by the Departmental Record Officer.

61. Information Managers are responsible for:

- designing, operating and maintaining a file plan covering for all records held by the business unit, irrespective of the media on which they are held;

- publicising the local file plan within their unit, so that staff know what needs to be kept, and where to store it;

- applying a unique file number reference, appropriate metadata, and a retention schedule to each class and folder (electronic environment) and each registered file (physical environment), setting appropriate permissions, and assigning an owner to assist with the eventual review and disposal;

- ensuring the unit's records are being properly stored in the appropriate folder;

- ensuring that registered files are clearly marked with the appropriate security classification;
- consulting the DRO if any registered files are missing;
- ensuring that records are only transferred between folders or registered files if they have been misfiled;
- ensuring that records are properly managed within the creating business unit through life, or until responsibility for those records is formally passed to a superior or successor unit, to Defence Business Services, or to another Government department;
- consulting the DRO when folders/registered files are transferred to another unit;
- closing folders / registered files, and capturing relevant metadata, on a routine basis as triggered by any of the following criteria:
    - action on the subject covered by the folder has come to an end;
    - nothing has been added to the folder for the last year;
    - the folder contains 100 enclosures;
    - the folder has been open for 5 years;
    - annually on 31 December (electronic folders);
    - the physical folder is 1 inch thick (paper folders).
- opening new folders (or folder parts) when, and only when, there is need to declare new records;
- undertaking regular reviews of the reviewing the contents of closed folder parts takes;
- ensuring that records of key folders are not destroyed;
- consulting the DRO's staff before any disposal action;
- ensuring that folders / registered files containing TOP SECRET records are not destroyed locally. Custody of all TS folders must be passed to Defence Business Services (Records Review team) as soon as they cease to be of business use;
- ensuring that there is no weeding of folders / registered files (i.e. no removal of individual records – the weeding of folders is prohibited);
- ensuring that folder level metadata is retained even after a folder part has been destroyed, for a minimum period of 20 years;
- making entries in the records management system for material that needs to be tracked as a record, but which cannot be stored directly in that system (perhaps because it is not in electronic form).

62. All Defence Staff are responsible for:

- keeping accurate official records;
- preparing records correctly for storage. Self-modifying fields (such as those that display 'current date' whenever the file is opened) should be replaced by fixed data as at the time the record is being created. Records should not be encrypted, compressed, password protected, or in any condition that will make them difficult to

access by authorised people;

- storing records correctly in the right shared areas in accordance with unit guidance. Electronic records must not be stored offline on media such as CD, DVD, portable drives, etc.

List of document types which must be preserved as records

63. There are some document types which must be preserved as records. These are documents which:

- contain TOP SECRET or Codeword material;
- contain information on important scientific or technical developments;
- are used by Official Historians or marked for retention by them;
- illustrate the formation and evolution of Defence Policy;
- illustrate significant developments in the relationship between the MOD and other parts of government, or other national or international authorities;
- show the authority under which the MOD has exercised a function;
- contain important decisions relating to the organisation, disposition or use of the Armed Forces;
- describe the reasons for important decisions, actions or provides precedents;
- could help the government to establish, maintain, or control a legal claim or a title;
- reflect Law Officers' opinion on any subject;
- establish committees, working parties or study groups, or which contain the proceedings and reports thereof;
- introduce (or consider introducing) new types of weapons and equipment, or modifications to them;
- discuss important trials and exercises;
- introduce new types of uniforms, clothing etc;
- concern the formation, organisation, reorganisation, re- designation or disbandment of units;
- concern notable legal matters;
- concern the occupation of historic buildings and sites of archaeological interest;
- relate to matters of general international, national regional or local interest which are unlikely to be documented elsewhere;
- contain reports of significant operations, intelligence, organisational and logistical matters;
- contain Histories produced by Service units etc;
- relate to Standing Orders and similar instructions of Commands, Agencies, Establishments etc;
- contain diaries, journals, logs, etc. providing an insight into particular operations or activities of wide interest.

JSP 441

MANAGING INFORMATION IN DEFENCE

PART 2 - GUIDANCE

JSP 441 – MANAGING INFORMATION IN DEFENCE

Overview

1. This is JSP 441 Part 2. It provides guidance on managing and using information effectively, so that we can meet our policy set out in JSP 441 Part 1. The JSP is sponsored by CDIO as the Defence Authority for Information, and the CDIO's foreword is in Part 1.

2. JSP 441 Part 2 covers a range of Information-related topics, including:

- standard data items used across Defence, that underpin many of our core systems;
- the ways we store, share, protect and preserve information, so that we work smoothly across Defence, and through time, effectively and efficiently;
- how we organise at unit level to provide effective information governance;
- how to manage records properly, to ensure that Defence is able to meet our obligations under the Public Records Act;
- advice on proven ways of making good use of our collective knowledge, that which we know but may not have written down.

3. It is published in the form of topic-based Guides, hosted on the Defence Intranet.

- Most of these guides are fairly short, designed to be read in a couple of minutes to improve the way that you and colleagues work with information;
- Some guides are much longer, cover detailed processes, and are aimed at information specialists. They are only likely to be needed if you are dealing with that specific issue;
- There will also be a collated version of all the guides, enabling you to search across the whole document.

How to use this JSP

4. You should familiarise yourself with the general guidance that covers the way that we handle recorded information in our daily work, for example how we should work with email and calendars, and how we name documents.

Further Advice and Feedback

5. Feedback is welcomed. Please contact CDIO's Information Policy team via this group mailbox.

Contents

Information

Records

Knowledge

Data

USING ELECTONIC CALENDARS

Overview

1. Most electronic office systems allow users to enter details on a calendar, and then make that information available to other users. It is the ability to see what other people are scheduled to be doing at any particular time, and for others to see what you are scheduled to be doing, that makes shared calendars such a valuable tool for effective collaborative working.

What you need to do

2. Keep your online calendar up to date, showing where you are, and displaying any scheduled events. If you don't do this, people are likely to assume that you're at your normal place of work.

3. Make your calendar available for all to read (see below for possible exceptions). Calendars are normally visible only to people on the same IT system.

4. Think about whether you want other people to have full or partial update rights to your calendar (typically used by senior officers and their personal staff). Make sure you understand what it could mean for access to the rest of your mailbox. Refer to the relevant User Guide to find out more about the calendar tool you're using.

5. Where event information is sensitive (or simply private), you should record it in such a way that the details are not visible to viewers, though they can see that you are committed. This is easily done on most calendar systems, but if not, just mark the event as a "Private Appointment". **However, sensitive personal data must not be included with calendar entries.** You should never include such things as staff reports, medical conditions, welfare reports, or anything that falls under the Data Protection Act definition of sensitive personal data (www).

6. **Don't put protectively marked information (including documents) in your calendar.** Instead, store it in a site with appropriate access controls, and provide a link to it from the calendar. Assuming the site access permissions are set correctly, the people who should be able to see the information will be able to. Doing this also helps to keep your mailbox size down.

7. Where you have more than one online calendar (such as role and personal calendars in DII(F)), you must use the calendar defined as "primary" for the system you're using. You should mark secondary calendars so that people checking your availability know where to look for your primary calendar.

8. Use the calendar system when inviting others to scheduled events (but if in doubt that you are using the other person's correct calendar, check by other means).

9. Keep significant events on your calendar after they have occurred, as they provide a useful record for you and colleagues, but delete the trivial.

10. Delete large attachments from historic calendar entries (or move them to the appropriate shared area, and replace by a link).

11. There may be good reasons, in particular security, for not making calendars of certain individuals, or indeed an entire unit, open Defence-wide. Restricting access to calendars is however a decision for the local command, not individual users. As always, sound judgement is needed.

MANAGING EMAIL ACCOUNTS

Overview

1. Electronic mail (or email) is a way of creating, sending, receiving and storing messages in electronic format, across an electronic communication network. Email applications enable us to communicate quickly and easily, irrespective of physical location. They also enable us to group correspondence by date, by sender, by subject, etc. Emails can be used both for informal person-to-person messages, as well as for the transmission of important corporate information across a wide audience. They are fundamentally the same as any other official document, and so need to be managed in line with relevant legislation and Departmental policies and rules.

2. We all need to use email wisely. Experience, not just in MOD but throughout the world, tells us that the freedoms offered by email come at a price. For all of the potential benefits, it doesn't take much to transform email from a useful tool into a significant overhead and threat to the business. Usage can be ill-disciplined and overly informal, and it is all too easy for people to send information via email, without thinking about the potential consequences. When you send an email, you lose control of the information you send. Information of all kinds – from the sensitive to gossip and trivia – can be transmitted to an audience far bigger than the one the initial sender envisaged, in a matter of seconds. Furthermore, because it is so easy to use and abuse, email triggers other problems too, such as:

- placing unrealistic demands on people - information overload, for example;
- time wasting;
- the distribution of computer viruses and other unwelcome material – unsolicited mails (spam), and offensive/inappropriate content of all kinds, etc.;
- confrontation;
- indiscipline and shoddy work - poor quality content;
- compromised security and privacy;
- inappropriate use;
- storage of important corporate material in private email libraries – this is perhaps the most prevalent of all these problems.

What you need to do

3. Always:

- set up your email account so that your email template includes your contact details (name, rank, post / job title, address, phone (internal & external) as a minimum) in what people often refer to as a signature block; you can easily remove the defaults from individual emails if you don't need them, or adjust them as required;
- set up your email account so that messages you send are automatically saved;
- avoid using scanned signatures – not only do they take unnecessary space, but they are readily copied and increase the chance of misuse;
- avoid setting up automatic Read and Delivery receipts (only use them when you really need to);
- organise and manage your emails properly; don't allow dozens, certainly not hundreds, of emails to accumulate in your Inbox;
- store emails containing significant information in the correct shared storage location (eg team sites, EDRMS, shared drives), not just in your personal storage – you should always do this when you send material, but do it for emails you receive as well (or ensure that someone else has done);
- deal with offensive or unwanted mails immediately;
- ensure that you have cover for incoming emails when you are away from your system (and allow for unexpected absences as well as the predicted) - set up at least one other person as a delegate with permissions to read your Inbox.

Handy hints and tips

4. You should:

- avoid indulging in lengthy email exchanges which add nothing to your work;
- not ignore email you receive that was not meant for you. Reply to the sender informing them that the email was incorrectly addressed and then delete the email;
- decide whether the email needs to be placed in shared storage (and unless the information in it is just trivial or transitory, then it probably should be – see ***What is a Record?*** If it's not worth saving in the corporate area, either delete, or keep it temporarily for your own benefit in your personal email folders.
- carry out housekeeping, managing your email account on a continuous basis, checking, deleting and moving items as necessary, and saving; in Outlook, for example. The key folders to check are as follows:
  - Inbox: it is good practice is to set a target number for the number of emails stored here (zero for the really keen, twenty is more realistic for most), and aim to reach it at least once during each working week. Do not use your Inbox as a general filing cabinet or a pending tray;
  - Draft Items: you should finish, file or delete items stored here, as soon as you can;
  - Deleted Items: set your email account so that it automatically deletes the contents of this mailbox when you exit Outlook; and
  - Sent Items: items not placed in shared areas or Outlook folders should be deleted regularly (keeping perhaps a month's worth of outgoing email).

5. When you know that you are going to be out of the office:

- turn on your Out Of Office Assistant for all planned periods of absence (more than, say, half a working day). However, be careful what you put in the message, as it will be returned to every sender who successfully emails you, including from the Internet. If there is information that you want MOD people to know, but not be automatically sent externally, then place the detail in your Calendar and refer readers accordingly (note – some systems, but not Outlook 2003, support separate internal and external messages);
- ensure at least one person, preferably more, has permissions to read your Inbox (this should be standard procedure anyway, to cover unexpected absences), and brief them accordingly;
- if the system permits it, consider setting up appropriate rules for handling messages of particular types, and reporting back to the sender;

6. Careless disclosure outside MOD of your email addresses or those of your colleagues can herald an increase in the amount of unwanted mail received, so where practical:

- only give email addresses to responsible third parties and where a legitimate need exists;
- where email addresses have to be in the public domain, consider setting using sacrificial addresses that can be abandoned if spam makes them unusable.

7. If you manage people who use email facilities:

- make sure they're sufficiently trained to do so. If they're not, make sure they get trained;
- make it clear to them that they are responsible for their behaviour when using email facilities, and for the quality and content of their emails;
- ensure they have read and understood the guidance in this document.

Other References

8. See the Guide on ***Sending, Receiving and Storing Emails***. Also refer to the User Guide for the system you're using.

SENDING, RECEIVING AND STORING EMAILS

Overview

1. This guide should be read in conjunction with ***Managing Email Accounts***, which provides an overall view of good (and not so good) practice with email.

2. Every time that you write email on MOD systems, you are creating a document that might be seen not just by the intended audience, but by others as well – once you've hit that send button, you've lost control on where it ends up. Everything we do is subject to the law (including the Freedom of Information Act). Always be professional - never write anything that you wouldn't be happy to defend in public if you had to.

What you need to do

3. Always:

- ensure that you label sensitive information appropriately, in line with MOD guidance on Government Security Classifications. Documents within Official classification don't need labelling, unless they are Official-Sensitive. Secret and above must be clearly labelled to ensure the reader knows its sensitivity. The protective marking should be that of the highest protectively marked material included in the email, **including** attachments (hyperlinks to protectively marked material not included in an email do not affect its protective marking);
- remember not to store or transmit emails on systems that are not cleared to the appropriate security level;
- be aware of privacy issues; use the facilities within the email application (such as Outlook, where you can set a Private option) to make sure that any private material can only be seen by the intended recipient (and not other people who may have delegated privileges);
- give each email you send a meaningful title, complying with the standard for ***Defence Document and Record Naming***, which includes the date of transmission and the appropriate protective marking (the date is included, as otherwise that important information can be lost when the email is moved between different storage environments);
- avoid using scanned signatures – not only do they take unnecessary space, but they can also be easily copied and misused;
- ensure that you address emails correctly; it is easy to get addresses wrong whether you are using role-based or name-based addresses;
- handle all information contained in emails you send and receive in accordance with the law and MOD policy. For example, don't use copyrighted material without proper permission, and make sure that you adhere to MOD's Acceptable Use Policy;
- take responsibility for the storage, quality, security, publication, availability and accessibility of any emails you send or receive;
- be sure that you have the appropriate authority (particularly if you are writing outside MOD, and especially on commercial matters) – the same principles apply as on signed documents;
- store emails containing significant information in the correct shared storage location (eg team sites, EDRMS, shared drives) – you should always do this when you send material, but do it for emails you receive as well (or ensure that someone else has done);
- avoid using offensive or inflammatory language, and especially anything that might be considered abusive, libellous or harassment; always be efficient and professional when you write emails;
- deal with offensive or unwanted mails immediately. Refer to relevant How To Guide;

Handy hints and tips

4. When writing emails:

- make sure your email is good enough for the intended audience. Good English still matters – check for grammatical errors, spelling mistakes, lack of clarity, logic – just don't agonise too long over the detail;
- make your email accurate, brief and clear;
- don't try to cover too many issues in a single email. One is usually best – but this may not always be possible or sensible;

- don't use email for the sake of it, and only send emails to those people who need to see them; in particular, avoid inundating more senior people – they may be interested in the final result of some collaborative work, but not in every twist and turn along the way;
- avoid using language that could easily be misinterpreted by the recipient (attempts at humour are usually best avoided, and sarcasm should never be used). However, there is nothing wrong with making the style interesting, engaging, friendly or personal, if that fits the purpose of the email;
- avoid overusing highlights - capitals, bold font, underlining etc – just because you can. These can distract;
- include hyperlinks (shortcuts) to related information where you can, if you are confident that the people you're sending the email to will be able to open them, and where the linked material is unlikely to be moved; excessive use of attachments clogs up network bandwidth and storage. Some systems prevent people reading or sending emails if their mailbox is above a given size, so help your colleagues by using links;
- include your key contact details (name, job title, office address, contact telephone number(s), etc) as appropriate – say, for example, when sending a note from a group mailbox or when writing to people who don't know you well). Guide ***Managing Email Accounts*** gives further details of how to set up a signature block, and what to include;
- if you're sending emails to a recipient list when some people can use the links, and some can't, then send it as two separate emails;
- send what matters and always consider your audience. Only send emails to those who need to be emailed; some people are so inundated by emails that it becomes impossible for them to be effective in their primary task;
- avoid using a distribution list as a 'catch all' when you only want to address a sub-set of the group;
- use the importance rating to your outgoing emails, where appropriate, but don't overuse high priority, as your recipients will soon learn to disregard it;
- don't send mass emails when you have other channels, like team sites and the Defence Intranet available;
- avoid including anything (for example, large attachments, badges, crests, backgrounds etc) that you don't need to – keep email size small and don't clog up bandwidth and storage. Badges and crests might be important when writing to people outside MOD, but aren't often appropriate for internal correspondence;
- if an action or response is essential, make sure your email has been delivered and seen by the recipient, and allow for transmission delays and breaks when sending between networks. You can't guarantee that an intended recipient has received an email you've sent;
- use the available IT facilities and tools where you can – spell checkers are particularly useful, but don't assume that they will automatically give you the word you wanted;
- unless you are working in a specialist area, such as legal or commercial, where disclaimers are necessary, don't use them – they have no real value and just clog up the email; avoid using other little tag lines as well, (such as "Save a tree - don't print");
- never have an argument via email if you can avoid it, and remember that embarrassing emails have a habit of getting forwarded widely;
- pause before you press the send key, and review what you've said. Are you giving the right message in the right way to the right recipients?

5. When sending an email:

- always think before you send. Could you justify the contents if it became public? Are you breaching any security or privacy constraints?
- copy it to the right people – don't send it to people who don't need to see it;
- if you don't need to keep a copy of the particular email, don't do so – it's usually a matter of clearing a check box;
- if you have kept a copy of the email, remember to save it in the proper place (see below for saving emails);

- be careful when using someone else's distribution list for non-MOD distribution lists, and check that the person is happy for you to do so. Inappropriate use of lists containing external email addresses could be considered an offence under the Data Protection Act 1998;
- be aware that the person at the other end will not necessarily read and action your email immediately; emails can be delayed in transit, especially between networks. Even if the recipient is there, he or she might have other priorities at that time – if urgent action is required, you might want to include that in the title line, but you'll probably need to phone as well;
- when sending an email over the Internet, take extra care that you are saying the right things to the right person at the right address. Never send classified information over the Internet – it is not secure, and there is a high risk of it ending up in wrong hands.

6. When receiving emails:

- Be careful when opening and reading the ones you receive. Watch out for suspect emails. Think about switching off your preview pane facility, so that you don't inadvertently open a suspect email by mistake when launching the email application (eg Outlook). If you're convinced that an email is safe to open, make sure you check the contents before deciding what action you need to take. It's impossible to make sensible work related decisions without doing this. Don't use auto-delete facilities, because you risk deleting something important that you need to be aware of;
- prioritise your incoming emails - you don't have to deal with all emails the moment they arrive, but ensure those that do require urgent action are dealt with promptly;
- if you receive a document with a working link, but which has the attachment as well, then remove that attachment;
- inform the sender when their message is unclear in any way;
- avoid indulging in lengthy email exchanges which add nothing to your work;
- if you receive email that was not meant for you, do not ignore it. Reply to the sender informing them that the email was incorrectly addressed and then delete the email;
- if you receive spam messages, don't reply, as you'll only get more – if you're being inundated with spam, report it to your iHub or the SPOC;
- decide whether the document needs to be placed in shared storage (and unless the information in it is just trivial or transitory, then it probably should be – see Guide ***What is a Record?***);
- if it's not worth saving in the corporate area, either delete, or keep it temporarily for your own benefit in your personal email folders;
- check the distribution – does the document need to be seen by colleagues?

7. When saving an email into corporate areas:

- choose the appropriate shared location;
- amend the email name if necessary to ensure that the title is meaningful, and accords with the Defence Document and Record Naming Standard (this includes removing any email prefixes such as RE: or FW (see Guide ***Defence Document and Record Naming***);
- update the metadata if necessary, to support searching;
- save the email, in its original format to ensure that its integrity remains intact (typically for Outlook as a .msg file, which will retain the attachments);
- be aware of any copyright issues – don't save copyrighted material into shared areas without authority.

8. When replying to, or forwarding, emails:

- think carefully before hitting "Reply to All", especially when there is a large distribution list … if all those people don't need to see your reply, then don't send it to them;
- only use as much of the previous text as is necessary to ensure recipients can understand the issue;
- don't forward attachments unless necessary – if you have saved the incoming email or its attachment into shared storage, send the link instead;
- think when forwarding an email – would the original sender have written the document in that way if he or she knew that it was going to the new set of recipients?
- be aware of any copyright issues – don't forward copyrighted material without authority.

9. Printing:

- as part of the MOD's Sustainable Development policy, unnecessary printing of emails (and other electronic documents) is discouraged – MOD manages waste according to the waste hierarchy (reduce, reuse, recycle) so better to reduce the waste by not printing in the first place.

10. The following summary of key points may be helpful:

- Consider alternative comms (eg Phone/Chat)
- Sort quickly (read, action, delete or file)
- Avoid multiple addresses (cc/bcc)
- Use naming convention and relevant subject in subject line
- Attach contact details

USING GROUP MAILBOXES

Overview

1. A Group Mailbox is the same as any other mailbox, except that it is intended for team use, not just (or even primarily) by one person. It can be used for incoming and outgoing messages, and can have its own folder structures (although these are not necessarily encouraged).

2. A Group Mailbox enables all business communication for a team to be received into, and dispatched from, one account. This not only offers greater control and visibility of all documents relating to a team's business, but is also an efficient method of covering for staff absences, or supporting round the clock operations.

Why and when you use Group Mailboxes

3. The choice to use Group Mailboxes is at the discretion of local management. For watchkeeping and similar activities, then they are the obvious choice; they also work well for the outer offices of senior officers. For other environments, the choice is not always so clear cut, but they should always be considered as an alternative to using individual mailboxes (person or role).

4. The use of Group Mailboxes complements, but does not replace, the use of proper shared corporate storage areas (EDRMS, document libraries in Team Sites, shared drives, etc.). Significant incoming and outgoing messages should be stored in these corporate areas, not in a folder structure within the Group Mailbox. In other words, the same principles apply to Group Mailboxes as to personal or role mailboxes.

Disadvantages of Group Mailboxes

5. The disadvantages of Group Mailboxes are fairly minor, and should not be regarded as reasons not to use them, more as a reminder to set appropriate local working practices:

- Team members must monitor Group Mailboxes, as well as their own;
- Replies to messages sent from individual addresses will almost invariably go back to the account from which they were sent, irrespective of whether the original message included a request to reply to the Group Mailbox. If you want replies to go to the Group Mailbox, then the initial message has to be sent from it;
- Messages sent from Group Mailboxes, particularly those from the outer office of a senior officer, can be seen as taking on a level of authority rather higher than may really be appropriate.

Managing Group Mailboxes

6. A Group Mailbox must have a nominated owner (and deputy) responsible for actively managing the mailbox on behalf of the business area. Their responsibilities include;

- making sure emails (inbound or outbound) are properly dealt with and then correctly filed in the right shared area;
- sending links to the people who need them;
- making sure that the list of people with access to the mailbox is kept up to date. It is every bit as important to remove access from those who no longer need it, as it is to add new names to the list.

Alternative to Group Mailboxes

7. Members of a team can make their own inboxes open to their colleagues. This means that each person's inbox can be monitored when they are away (note that some MOD systems require the entire mailbox, including folders, to be open, and cannot leave just the inbox accessible). This is good practice, irrespective of whether a Group Mailbox is used, although it runs the risk that sometimes messages will be more widely visible than the sender intended.

STORING AND FILING INFORMATION

Overview

1. Storing and filing documents correctly makes them easier to find again. Many of our documents (especially those related to operations), need to be kept for many years; it's important that we store them in such a way that others can retrieve them. By document, we mean any of a wide variety of electronic file types such as word-processing files, text files, spreadsheets, presentations, drawings, databases and emails (the same principles apply to documents on paper or other media too.

2. To help people (now, or perhaps well into the future) to find the document they are looking for among the many millions that MOD generates, we need to label them properly, and store them in the right place. Labelling documents is covered in Guide 999, Labelling Information, while Search techniques are covered in Guide 999, Searching.

3. MOD systems use a range of technologies for storing information: intranets, EDRMSs (such as Meridio), team sites (SharePoint / MOSS), shared drives, personal file store in My Docs and Outlook, and others.

Storing Significant Information

4. It is vital to ensure that significant information is stored in the right shared areas (where the shared area may be the EDRMS, a team site, or a shared drive. This enables us to:

- Keep related information together for easy browsing and searching;
- Make the information available to those who should have access to it;
- Protect it from those not authorised to have access;
- Preserve it for an appropriate period of time.

Managing Shared Areas

5. Information Management professionals within each organisation need to structure the shared areas properly, whatever the technology, to ensure that these conform to the overall policy and with the needs of the business unit they serve. It is then up to all of us to use them well.

6. File plans (or file lists, as they are sometimes called) show how a registered filing system is organised. The structured file plan approach is usually associated with maintenance of the Defence Record and the basis of the Department's registered file system, but the same principles apply to all information, whether or not it is likely to end up as a formal Departmental Record.

7. File plans are generally hierarchical in paper systems, in an EDRMS, or in shared drives found on Microsoft systems and others. They lend themselves to an overall Defence-wide structure, whereby similar plans can be used across large numbers of units (for example, all ships could use a standard structure). Team sites are somewhat different, as they are usually formed around the needs of a particular group – the important thing is to tie the document libraries within team sites to an appropriate class or folder within the hierarchical file plan.

What you need to do (applies to all users of MOD systems)

8. These few basic rules will help you, your colleagues, your successors, and the MOD generally:

- ensure that you understand the way that shared storage areas are used within your unit;
- understand where existing information related to your work can be found, and where new information can be stored;
- use the shared areas for all information of significance, seeking advice from the Information Professionals within your organisation where necessary;
- ensure that the shared storage areas provide appropriate access to those who should see them, but not to those who shouldn't;
- label documents properly using the MOD naming convention and using metadata
- ask the Information Professionals in your unit whenever you need to set up new team sites, document libraries, folders (or other shared areas).

Please note. Keeping important MOD information in My Docs or individual email accounts is a bad idea – it stops us from sharing, protecting and preserving information effectively. It also makes it much harder for MOD to comply with legislation (especially Public Records Act and Freedom of Information Act).

What Information Professionals need to do (SIOs, IMgrs, ISOs and ISAs)

9. The task of the Information Professionals is to ensure that all information within their business unit is correctly stored and labelled, shared, protected, and preserved. You should:

- ensure that you understand both the overall policy, and how it is to be applied in the systems you are using within your unit;
- understand the needs of the business that you are supporting;
- ensure your file plan is properly structured;
- ensure that all titles of information containers (classes, folders, files etc.) are meaningful, with relevant subject category or categories taken from the UK Defence Taxonomy (MOD) and, where relevant, the UK Defence Thesaurus (MOD);
- ensure the appropriate security, privacy and accessibility of information through appropriate use of privileges;
- educate your business community in the proper way to use the system, and monitor that they are using it properly; and
- ensure that senior management understands why proper organisation of information is important, and that their leadership role is critical to success.

LABELLING DOCUMENTS

Overview

1. Labelling documents well makes them easier to find again. Many of our documents (especially those related to operations), need to be kept for many years; it's important that we store them in such a way that others can retrieve them. By document, we mean any of a wide variety of electronic file types such as word-processing files, text files, spreadsheets, presentations, drawings, databases and emails (the same principles apply to documents on paper or other media too.

2. To help people (now, or perhaps well into the future) to find the document they are looking for among the many millions that MOD generates, we need to label them properly, and store them in the right place. Storing documents on DII is covered in Info Guide 05 ***Storing and Filing Information***, while Search techniques are covered in Info Guide 09 ***Searching for Information***.

3. This guide covers two complementary approaches to labelling:

   a. Document and Record Naming – the use of standard names for documents;

   b. Metadata – adding properties to documents that can easily be found by search engines.

Document and Record Naming

4. MOD has a mandated standard for document naming (which of course applies to records) as follows:

Date–Title–Protective Marking

5. As well as getting the format right, it is important to make the Title meaningful. Details on the Document and Record Naming standard, are in Info Guide 07 ***Naming Documents and Records***.

Metadata

6. Metadata means 'data about data'. It can be applied to information held in many formats (such as a hashtag in a tweet, or the notes people write on the label of a CD case), we generally use it to help in management and retrieval of electronically held documents and files.

7. MOD uses a controlled vocabulary known as the UK Defence Terminology. This consists of two elements – the UK Defence Taxonomy, and the UK Defence Thesaurus. Both of these are available on the Defence Intranet.

The Defence Taxonomy

8. In standard English, a taxonomy is a scheme of classification. The term originated in biology, and was used for the classification of living species. These days, it is used much more broadly, so a taxonomy is a system for naming and organising things into groups that show similar characteristics. The Defence Taxonomy does just that for words used within Defence. It is the approved and authoritative list of Defence subject categories, structured to reflect all the main business activities undertaken across Defence. It helps with the naming of electronic folders and file names with relevant and meaningful subject categories. It is updated annually. Use it to identify the appropriate subject or subjects to describe your information.

The Defence Thesaurus

9. A Thesaurus is a publication which groups words together if they have similar or related meanings. There are several well-known published thesauri (or thesauruses) such as Roget's and Oxford, and the word processors usually embed a thesaurus to enable their users to find synonyms, or just a better word for what they are trying to say. The main purpose of the Defence Thesaurus is to show the Defence preferred term for any particular subject, rather than any of the many alternatives that standard English allows.

10. The Defence Thesaurus supports and expands on the Defence Taxonomy and is the approved, authoritative list of subject keywords that you should use to describe your documents. It follows the principle 'one concept, one term', and directs you from non-preferred terms such as synonyms and abbreviations to preferred ones. It also provides subject keywords for each top-level Taxonomy subject category, and offers keyword metadata values to help describe content. Use these controlled vocabularies whenever you label documents using metadata.

What you need to do

11. You should:

- adhere to the **Defence Document and Record Naming Standard** when you name a document (including records);
- give information resources meaningful titles. Label all electronic folders or documents, irrespective of the system you're using, with relevant subject category or categories taken from the UK Defence Taxonomy (MOD);
- add useful metadata to the document by selecting valid keyword terms from the UK Defence Thesaurus (MOD).

Handy hints and tips

12. Here are some useful ideas to consider:

- you're trying to help people find information in the future, so think hard how best to do this. Try and anticipate obvious words they're likely to use when searching for material such as the ones you're describing. It's important that you adhere to the naming standard and do your best to add useful metadata. These things are important;
- get to know the preferred terms for your specialist area of work;
- be as specific as you can be with the terms you use, but recognise that there is no perfect solution;
- look out for opportunities to improve the Document and Records Naming Protocol, Taxonomy and Thesaurus;
- consider producing your own lower level guidance, where necessary, but make sure it doesn't contradict or conflict with the departmental policy and standards referred to here.

13. Labelling is about being tidy. It might take a bit of extra time when you first store a document, but it pays dividends in the long term. Your work is important – make it easy for other people to find it when they need to.

NAMING DOCUMENTS AND RECORDS

Overview

1. Naming documents clearly makes it easier to find them, and using a standard naming convention across Defence is more sensible than everyone having their own.

2. There are mandatory components, each separated by a hyphen:

- **Date** and **Title** apply in every case
- Where a document has a security marking of OFFICIAL-SENSITIVE, or is classified SECRET or TOP SECRET, then there is a third mandatory component of **Marking**.

What you should do

3. Name documents (such as word-processing files, text files, spreadsheets, presentations, drawings, databases and emails) this way:

Date–Title (for OFFICIAL)

Date–Title–Marking (for OFFICIAL-SENSITIVE and above)

- Only the following characters are normally allowed: A-Z, a-z, 0-9, hyphen, round brackets, space, underscore.
- Some TLBs say "Don't use spaces, use underscores instead"
- Avoid using any of these characters: ~ # % & * { } \ : < > ? / + | "
- **Date**
  - Written in format YYYYMMDD (e.g. 20151013)
  - Optionally, and if it's important, you can add time (and zone) after an underscore (e.g. 20151125_0930Z)
  - Use the date that you're creating, or amending, the document (i.e. today)
- **Title**
  - Make it meaningful and concise – use spaces or underscores to separate the words, avoid unnecessarily long file names as these can cause trouble
  - Add any of the following if it helps clarity, or if it is your TLB standard:
    - Document status (e.g. DRAFT, FINAL)
    - Version in form vx_y (eg v2_5)
    - Originating unit or role
    - File Reference
  - For emails only, if there are any special handling instructions, these should be referred to within the title (see GSC Survival Guide)
- **Marking**
  - Use one of the following abbreviations for OS and above

    OS (for Official-Sensitive)
    S (for Secret)
    TS (for Top Secret)
  - If there is a descriptor, you should add it after the classification

    PERSONAL
    COMMERCIAL (can abbreviate to COMRCL)
    LOCSEN (not accessible to locally engaged staff overseas)
    LIMITED CIRCULATION (see JSP 440 Chapter 4-1-2)

Examples

4. Here are two examples, one with the basic terms only, and one with some options:

20151114-Presentation on Government Security Classifications
20151126_1135Z-Jackal Maintenance Contracts DRAFT v2_5-OS COMRCL

KEEPING GOOD RECORDS

Overview

1. Record keeping is an essential part of working in Defence. It is vital – both in meeting Defence's Military Tasks and in all we do to prepare for and support those Tasks – that we are able to account for what we have done. Every Civil Servant is obliged to do so by the Code of Conduct, which says: "*You must keep accurate official records and handle information as openly as possible within the legal framework*". For Military staff, it is every bit as important; often the more risky and demanding the activity, the more important it is to have records to learn from, and provide explanation. This message has been reinforced very clearly from Iraq and Afghanistan, and we are now required to keep not just all records from theatre, but also for everything we did preparing for the operation. Keeping records should not be a burden, but an integral part of the way we work.

2. The aim of Records Management is to select and save records in such a manner that they tell the full story now, and will continue to do so in the future. Part 1 of this JSP – the Directive – contains specific Records Management rules that apply to all of us.

What are Records?

3. 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 units, working with their TLB and CDIO's Corporate Memory team, 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.

4. 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.

5. Any significant piece of work, such as documents which contribute to a decision, should be saved as records, as well as any correspondence sent externally. Documents produced regularly as part of an administrative or operational process (such as minutes and meeting papers, data returns, reports, Memoranda of Understanding, audits, etc.) may form an unbroken series of records and should be saved together as a group. Emails are documents – if they are in any way important, file them as a record, along with any attachments.

6. Any document which is subject to statutory or regulatory requirements, e.g. finance and accounting records, contracts and agreements, must be declared as a record and retained for the required period, as recommended by CIO Corporate Memory. Any item which may have legal, contractual or financial implications for MOD must be retained (and in certain circumstances, the original hardcopy must be kept as well).to meet legal and business requirements.

What you need to do

7. For all staff:

- understand why records are important, and do your part in helping to build the MOD's corporate memory;
- use shared storage areas (the right ones) for all your business-related work;
- label documents properly;
- follow instructions and advice from your local Information professionals; and
- **never** destroy information in such a way that your actions may be interpreted as an attempt to avoid disclosure of that information or to cover up something.

8. For Information professionals:

- follow the Records Management rules in Part 1 of this JSP, and the RM guides in this Part 2;
- understand the key points of the law, and comply with statutory requirements – Data Protection, Freedom of Information and Public Records Acts;
- use an record management system, and manage it well;
- give the hierarchy of document containers (team sites, libraries, classes, folders, files etc.) meaningful titles using relevant subject category or categories taken from the UK Defence Taxonomy (MOD) and, where relevant, the UK Defence Thesaurus (MOD);

- use the electronic systems to keep a register of your physical records, to make them easier to find;
- ensure staff in your unit use the shared areas properly, placing all relevant documents in the appropriate container;
- ensure significant documents are protected from accidental or deliberate deletion;
- define appropriate retention schedules. All records must be capable of being preserved, stored and reliably and securely retrieved over the required period to satisfy operational, business, legal, statutory, public and national requirements for the information which they contain. The required period of retention will vary according to the nature of that information;
- transfer appropriate files to CDIO Corporate Memory at the right time;
- regularly review your local records management policy, to ensure that it remains in line with Departmental policies and standards; and
- if in doubt, seek advice from your TLB or CDIO Corporate Memory.

SEARCHING FOR INFORMATION

Overview

1. Searching for information is fundamental to Defence business. The modern world presents us with a mass of information, and many and varied tools for looking for it. Good use of search techniques and understanding the information sources available will make you more effective in doing your job.

2. We're all familiar with the power of Internet search engines to find just what we are looking for, and usually on the first page of the results screen. Finding material in the MOD can often be trickier, and it helps to understand where and how information is likely to have been stored.

Information Sources

3. For MOD material, the following are the main sources of general information:

- The Defence Intranet contains the vast majority of formal published material including JSPs, DINS, News, departmental blogs, and forms. The Intranet is maintained by DBS KI, and all information posted should have an owner;
- DII Team sites are the main shared area for collaborative work, and they are controlled at unit level. Local iHub staff will be able to advise on the structure for a particular unit, and you will be able to access material from all other units, if you have the right access permissions (and many sites are open to all);
- Meridio (Electronic Management Records System), also controlled at unit level, contains material declared as records (which ensures that it cannot be changed, and will be subject to formal review at a time determined by the retention schedule) – again the right access permissions are needed;
- Group File Store (GFS) is a hierarchical storage area in DII, and was used for record storage before the widespread rollout of Meridio;
- Enterprise Directory contains information on people, and the posts they fill;
- Defence Connect (Jive) is an Enterprise Social Network, and contains information posted by people across Defence;
- The MOD Main Archive is housed at TNT in Swadlincote, and managed by DBS KI – it contains hard copy material (nearly all paper) produced by Defence units, where retention is important, but the documents are not in regular use;
- Library and Information Centres, also run by DBS KI, contain, or have access to, large volumes of information in various formats (including access to external electronic and other libraries) – they also offer expert advice.
- MOD publishes large volumes of material to the Internet; the major websites are MOD (on GOV.UK), Royal Navy, British Army, Royal Air Force;
- GOV.UK is the central site for rest of Government, while other public bodies with whom MOD works closely will host their own websites (such as The National Archives and the Information Commissioner);
- Public information from MOD and the Single Services is normally announced on Twitter (not available on DII), so offers an easy way to keep up to the minute with Defence news.

Guidance on Searching

4. We're all so familiar with the basics of searching, but it's helpful to read and understand the help pages on searching, both in MOD systems and in commercial search engines (so for Google Help, type Google Help). The following general advice is offered:

- consider the best way to search – using search engines, databases, library services. If unsure where to start, look within MOD first. Where specialised skills are required, seek help;
- describe in plain language what you are looking for, especially when others are finding the information for you;
- check the accuracy. Beware of bogus or biased information that presents a point of view rather than being accurate and independent.

- check the currency. When was it last updated? How current does the information need to be to suit your needs?
- check the content. How detailed is the information? Does it cover everything that you need? What evidence has been provided to back it up?
- check the source. Do you know who has produced the information? Do you know what qualifies the author to provide the information?;
- where possible find information from more than one source and compare them;
- build efficient search strings when searching web sites;
- use the 'Favorites' facility on your browser for sites (internal or external) which you visit regularly;
- balance the cost of searching for information against the value of what you want to use it for;
- much good quality information available on the Web is only available at a price, so consider whether the information is exactly what you require before paying. And before you commit to payment, check with MOD library services - they may already have an account;
- use local sources of information. Experts are usually happy to be asked, but they like you to make a bit of effort as well.

5. Finally, take care that the information you find is sufficiently reliable for your purposes. Where information must be correct, check the source, accuracy, currency, content, and where possible compare it with other sources. No source of information is infallible, but some are more reliable than others – use sound judgement in assessing the quality of information provided against the level of accuracy you need.

USING HYPERLINKS

Overview

1. Hyperlinks are links from one place in an electronic document, to another place in the same or another document; they are activated by clicking a highlighted word or graphic. They enable one master copy of a document to be published, with other documents (including emails) referring to it. That master copy can be properly stored, labelled, protected, preserved – this is why proper use of hyperlinks is strongly encouraged within MOD systems.

2. Hyperlinks have one great advantage, that can also be a disadvantage. The document to which a hyperlink will take the reader can be updated, without changing the hyperlinks, which is a very convenient way of presenting current information. But it has a downside – it is risky from a records perspective, as the information that was there may have been changed, unbeknown to the user. (Note – if you link to a document or record that cannot be changed, e.g. one declared as a Meridio record, then you get neither the advantage nor the disadvantage.)

When and how to use hyperlinks

3. In general, when you wish to refer people to a document (for example, minutes of a meeting, a paper for review, a financial spreadsheet, or a presentation), place the document in the appropriate shared storage area, and send them the link by email (or via an alert). If in doubt on how to do this, read your User Guides or Help screens – it's easy.

4. However, you need to be sure that your readers will be able to follow the link and open the document. In general, if people are on the same network, and they have the right security permissions, then they will be able to see the document; if not, you may have to resort to sending attachments.

5. If you are publishing a document to which readers will be referring by hyperlink, and you want to amend the document while leaving the links attached, make it clear on the document when and how you have changed it, so readers are not taken by surprise when the document no longer says what they thought it did.

6. Of course, if you move or rename the target document, the link will no longer work. Therefore hyperlinks work best when the need for them is likely to be short-lived.

7. Use hyperlinks in routine work – however, they are risky for records purposes, and the traditional attachment may then be necessary.

Absolute and relative hyperlinks

8. Understanding the difference between absolute and relative hyperlinks is important if you are moving files from one place to another, and wish to keep links intact. An absolute link specifies the exact location of the target document; a relative link tells you where it is compared to the current location. So for example, if you are writing a set of documents with internal links on your personal storage area, and then moving the entire set to a shared environment, then you should use relative links.

USING ELECTRONIC DIRECTORIES

Overview

1. Electronic directories are organized sets or collections of information, often about people, organisations and locations. A simple workforce directory will probably include the basics - names, post titles, work addresses, email addresses, phone numbers, etc. However, directories are often much more sophisticated than that, often offering specialist information such as job descriptions, skills profiles, location maps, etc., and a wide choice of display and search options. They are also at the heart of Enterprise Social Networks in modern office automation systems, increasingly the way that business gets done.

2. Electronic directories need to be well designed and managed, and only contain good quality (current, accurate, unambiguous) information. They also need to be quick and easy to maintain and use, otherwise people will lose confidence in the quality of the information held.

The MOD's main corporate directory

3. The MOD's main corporate directory of people and organisations is the Enterprise Directory (ED). The information held on the ED not only needs to be maintained, but it needs to be protected too. The MOD, for example, does not permit the production or distribution of off line copies of the directory, nor does it allow people to export significant amounts of bulk data from the ED.

What you need to do

4. So that everyone across Defence can benefit from a reliable directory, you need to play your part:

- familiarise yourself with the Enterprise Directory, and any other directories that you use for MOD work (including enterprise social networks such as Defence Connect);
- maintain the information for which you are responsible, keeping it accurate and comprehensive. If there are errors, get them fixed. If the information relates to another person, let the person involved know;
- avoid putting sensitive information on the directory – neither personally sensitive nor MOD sensitive;
- protect information appropriately, and don't misuse it;
- do not export information at all unless you have an exceptionally good reason to do so, and then ensure you follow the relevant rules.

HANDLING INFORMATION REQUESTS

Overview

1. Anyone can request information from MOD, and each is entitled to a reply. Whether they get the answer they requested depends on the question, and (in the case of personal information) who they are. It is essential that MOD handles Information Requests correctly. There is good advice available from the experts in handling requests, and links to their pages are shown below.

Types of Information Requests

2. The following are the major types of information requests:

- **Parliamentary Questions** (PQs). These can be tabled by Members of Parliament to seek information or press for action. All questions, whether transcribed from the Chamber or recorded from a printed format, are recorded in The Official Report (Hansard) and so they are widely available and accessible;

- **Ministerial Correspondence** (MC). These are letters addressed to Ministers, to which a Ministerial reply will be sent. The Minister's Private Office will allocate a responsible Division, and the deadline for the reply;

- **Treat Official (TO) Correspondence**. This is essentially correspondence to Ministers from members of the public. Each year Defence Ministers receive around 10,000 pieces of TO Correspondence. TOs get a response from the appropriate official in the division or unit responsible for the topic. The covering note from the Minister's office will inform whether or a letter (or email) is to be treated as TO or Ministerial Correspondence;

- **Freedom of Information (FOI) Requests**. The FOI Act places an obligation on public authorities to make information available on both a proactive and a reactive basis. The terms of the Act are broad: every written request for information from an identifiable person should be treated as an FOI request, even where the Act is not mentioned. A response must be sent within 20 working days;

- **Requests under the Environmental Information Regulations (EIR)**. These cover all requests for environmental information. Requests can be in written or in oral form (a difference from FOI), must have a name and address for communication purposes, and must be clear. As with FOI, the request does not have to mention the regulations;

- **Subject Access Requests (SAR) under the Data Protection Act (DPA)**. An individual (data subject) is entitled to request personal data held by MOD relating to him or her. Such requests are called Subject Access Requests (SARs). A response must be sent within 40 days.

- **Military Service Record Requests**. These are submitted to the appropriate authority on a form accessible through GOV.UK.

What you need to do

3. Be prompt, be professional, and familiarise yourself with the appropriate guidance. If in doubt, ask your local or departmental experts.

4. Before dealing with information requests you must familiarise yourself with the relevant Regulations and supporting advice available on the Defence Intranet, in particular:

- Parliamentary Branch advice on PQs, MCs, TOs;

- CDIO Information Rights team advice on FOI, DPA and EIR.

5. Requests received in the Welsh Language must be answered in Welsh (for examples of Welsh, see the Welsh Language Commissioner's website). If you need the request and response translated, contact CDIO Information Policy team.

6. For further details on the Freedom of Information Act, the Data Protection Act, and the Environmental Information Regulations, see the Information Commissioner's Website.

UNDERSTANDING SPECIALIST INFORMATION ROLES

Overview

1. Everyone in Defence has an important role in managing and using information effectively. Some of us are in specialist roles, with specific areas of responsibility. These roles are critical in helping Defence make best use of its information, and stay within the law. Some of these roles are in the various Headquarters, but most can be found in Units across Defence.

2. Each CIO-approved specialist information role has its own Information Role Definition setting out the main tasks involved. TLBs and units can adapt these templates to help them meet local requirements and cater for local priorities and constraints.

3. The skills requirements for the roles, together with details of the approved training options available, are set out in the Information Skills Compendium.

4. People can fulfil more than one role. They can also delegate responsibility for a role where it is sensible to do so.

Leadership, Responsibility and Accountability

5. The Defence CIO (now CDIO) is the Defence Authority for Information, appointed by PUS with responsibilities specified in the letter of authority. CDIO works with a network of TLB Chief **Information Officers** to help Defence achieve its information aims.

6. PUS also appoints the **Departmental Record Officer,** a role found in all Government departments. The DRO leads for Defence on compliance with the Public Records Act and is responsible for our relationship with The National Archives. A small number of specialist units have delegated DRO responsibilities.

Information Management within Units

7. The MOD mandates three core Information Management (IM) roles - **Senior Information Officer**, **Information Manager** and **Information Support Officer)** - within units. A unit may also employ **Information Support Administrators** within its iHub.

Risk Management and Information Assurance

8. **Senior Information Risk Owners (SIROs**). The CDIO is the SIRO for Defence, and delegates responsibility to a group of TLB SIROs.

9. **Information Asset Owners (IAOs).** All important information assets – whether they contain personal information or other critical information – must have an owner. This is policy which applies not just in Defence, but across Government. The role of the IAO, defined here by the Cabinet Office, is "to understand what information is held, what is added and what is removed, and who has access and why". The IAO is to manage risks to the information, and is to ensure that it is effectively used within the law.

Information Rights

10. **Data Protection Officers (DPOs).** CDIO's Information Rights team is responsible for overseeing the implementation of the Data Protection Act throughout MOD, and publish guidance. A network of Data Protection Officers at TLB/Agency level provide local advice and governance.

11. **Freedom of Information Focal Points.** CDIO's Information Rights team is responsible for overseeing the implementation of the Freedom of Information Act throughout MOD, and publish guidance. A network of FOI Focal Points across Defence provide local advice and governance.

Data Management

12. **Data Managers** are responsible for the management of structured data in their organisations. They report to their TLB's CIO.

13. **Data Owners** are accountable for the quality and availability of specific sources of data and Management Information.

14. **Data Stewards** support the Data Owners in their task.

Intranet Management

15. **Defence Intranet Managers** are responsible for the quality and publication of information on the Defence Intranet. This could be at TLB or unit level. **Defence Intranet Publishers** publish information on their behalf;

UNDERSTANDING THE ROLE OF iHUBS

Overview

1. MOD Policy requires that information should be managed at Unit Level. There is a standard structure, built around three professional IM roles (SIO, IMgr, ISO), and an organisation for conducting information administration (iHub).

2. Implementation of iHubs is the responsibility of TLBs. Although this guide describes a generic structure and set of functions, as well as guidance on determinants of their size and shape, iHubs must be designed to meet the diverse needs of units across Defence, and that expertise lies within the TLBs.

3. This guide:

- explains what iHubs are;
- defines the main roles and responsibilities;
- outlines the required skill sets for iHub staff.

4. The iHub is the focus for all Information Administration (IAdmin) at unit level, and underpins effective Information Management. The iHub's task is to ensure the effective receipt, storage, organisation, distribution, protection, preservation and disposal of information in the unit which it serves.

5. The iHub should be staffed with information professionals trained to support their organisation. The Head of the iHub is the Information Support Officer (ISO), and staff within the iHub are Information Support Administrators (ISAs). The ISO is responsible for carrying out the policies set by the Senior Information Officer (SIO) and Information Manager (IMgr), and is accountable to the Unit SIO and IMgr for all aspects of IAdmin.

6. The iHub concept is independent of technology and the work of the iHub will include activities in support of all information systems deployed in the unit.

Functions

7. The role of the ISO and iHub staff (ISAs) is to deliver efficient Information Administration to their unit, and in support of their SIO and IMgr. Teamwork across all the professional IM roles is critical, and some of the activities listed below (particularly those around communication with other members of the unit, allocation of responsibilities, and high level plans) will often be led by the SIO/IMgr.

8. Functions of the iHub will include:

a. Information Management Policy and Practices:

- advise all staff on IM policy and guidance, and use of the organisation's information systems;
- monitor information activities to ensure compliance with the law, and with MOD, TLB and Unit policy;

b. Correspondence management:

- act as a Receipt Despatch Centre;
- scan and register documents;
- maintain paper logs;

c. User Account Management in DII and other systems:

- create, amend and close user accounts;
- manage user privileges and profiles;
- monitor capacity;
- ensure mailboxes are being actively managed (including in absence of owner);
- undertake DII roles of Local Security Officer and Authorised Demander;

d. Management of Group Mailboxes (setting up, closing down, monitoring, distribution of messages);

e. Management of High Grade Messaging:

- manage the automatic distribution mechanisms (allocation of SICs);
- act as Guaranteed Action Point (GAP), ensuring High Grade Messages are addressed within timescale of precedence;

f. Document and Record Management:

- create and manage the organisation's file plan;
- create, maintain, and delete team sites and shared drive folders;
- establish and maintain appropriate access permissions to team sites and shared drives;
- set up default metadata in team sites and the Electronic Document and Record Management System (EDRMS);
- map team sites to EDRMS folders;
- establish records management folders in NTFS (or other file system) for units not equipped with EDRMS;
- undertake team site administration, or delegate authority to someone nominated by the appropriate Team Leader;
- maintain and promulgate record retention instructions;
- set retention schedules for all record holdings in accordance with JSP 441 (and with advice from TLBs and CDIO's Policy team as required);
- review record holdings in accordance with retention schedule, and with advice from appropriate unit staff;
- capture records from folders and team sites being closed;
- manage physical records (paper, CDs, tapes, film, etc) and their repositories;
- arrange the transfer of records to the appropriate authority, or their destruction/deletion, as required by JSP 441;
- create and manage local document templates;
- audit use of team sites, shared drives and EDRMS for duplicate data, redundant files not intended for records, team sites that are never used, etc;

g. Collaboration:

- set up online chat meetings, chat rooms, conferences and teleconferences (possibly in conjunction with service provider);

h. Operational Record Keeping:

- maintain and submit the Operational Record;

i. Information Retrieval:

- advise on use of internal and external information search facilities and library services;
- advise on use of controlled vocabulary, taxonomies and thesaurus;

j. Information Dissemination:

- manage organisation's Intranet sites;
- publish or forward messages received to appropriate staff;
- disseminate key information on behalf of owners;
- provide service for transferring information between different environments (eg to and from tactical systems, IMPEX);

k. Information Assurance:

- ensure that Information Asset Owners are allocated for all current and significant information for which the unit is responsible;
- validate, establish and maintain access permissions to information assets for external users;
- ensure information aspects are covered in business continuity plans;
- ensure arrangements are in place for security and protection of physical documents and information;
- assist in impact assessments relating to information damage or loss;
- manage and advise on the classification of folders;

l. Information Handling:

- ensure that the rules for the secure storage and transmission of information (in particular protectively marked material, and personal information as defined by the Data Protection Act) are widely understood and rigorously followed within the Unit;
- account for all portable media devices (including laptops, memory sticks and CDs/DVDs), and ensure their users are aware of the regulations;

m. Training and Education:

- ensure unit staff receive appropriate training in Information Management Policy and Practice on joining, and arrange refresher training as required;
- ensure unit staff are aware of key documents, in particular the Acceptable Use Policy (JSP 740) which applies to all MOD ICT, and the SyOPs and User Guides for the systems they use;

n. MOD Directories:

- maintain the organisational structure in Enterprise Directory;
- ensure unit staff maintain personal entries in Directories (in particular Enterprise Directory);

o. Support for, and advice to, Unit Staff:

- support SIO and IMgr in execution of their duties;
- advise all staff on the use of information systems within the unit;

- advise all staff on use of the applications available on DII (including Microsoft Office) and other systems;
- support unit staff in routine information management activity; and
- trouble-shoot as required (eg locating lost information or folders);
- undertake general administrative functions as required by local Command;

p. Point Of Contact for IS providers:

- provide the Local Point of Contact (LPOC) for resolution of IM problems on, or in direct support of, Operations and training;
- support the Theatre Point of Contact (TPOC);
- support the ISS Single Point of Contact (SPOC);

q. Operational resilience (deployed units):

- ensure the continuous availability of information to the organisation it serves through appropriate transfer of information, and control of local back-up devices.

Skill Sets

9. A range of information skills is required in iHubs. The breadth and depth will inevitably depend on the nature of the unit, the size of the iHub, and the information infrastructure in place. TLBs will set detailed requirements. Generally, iHub staff are expected to have a good understanding of:

- key elements of information legislation, in particular the Data Protection Act and Freedom of Information Act;
- overall MOD Information Management policy and guidance (JSP 441 Parts 1 and 2), Web Publishing Policy (JSP 745), and the Acceptable Use Policy (JSP 740);
- Information Security rules (JSP 440 and local instructions);
- information infrastructures (eg DII, BCIP) used within the unit, the means by which they are supported, specific constraints (such as bandwidth availability, file sizes and allowable formats), and the associated documentation (especially SyOPs and User Guides);
- Microsoft Office Applications (in particular Outlook, Word, Excel and PowerPoint, with a basic understanding of Project, Access and Visio);
- collaborative working tools and shared storage environments as used within the unit (eg Microsoft SharePoint, Meridio EDRMS);
- the MOD Information Management Maturity Model;
- the information services available on and through the Defence Intranet;
- TLB Information Management structures, contacts and instructions;
- Operational Record Keeping procedures;
- the unit's file plan and shared storage configuration (eg team sites);
- Principles of Information Assurance (particularly in operational theatres).

Implementation

10. The fundamental principle is one iHub per unit. Definition of what comprises a unit is determined by TLBs but essentially a unit will have its own address for messaging (the Electronic Unit Name (EUN) - the characters before the first hyphen in role-based emails), and its own shared storage areas.

Preparing for, and Recovering from, Operations

11. The most vital task of an iHub in a deployable unit is to ensure that the information needed by the Command on operations is available and properly administered. The iHub must be able to translate readily its information from barracks to the field, and from DII (or other fixed infrastructure) to deployed command systems. The golden rule of 'organise for Operations and adjust for barracks' should be followed. On return from Operations, information will need to be migrated back to the main infrastructure used at the home base.

Size and Shape of iHubs

12. The table below indicates the main factors to be considered when designing the iHub model for the organisation:

Factor	Considerations
Level of IM Maturity of the organisation	Low Level of IM Maturity – drives a centralised model of iHub which can maintain tight control of information structures and behaviours. High Level of IM Maturity – would enable a federated model to be employed.
Geographical spread of the organisation	Low Geographical spread – would suggest a centralised model of iHub. High Geographical spread – would favour a more federated model to ensure that iHub staff are located closely to the users they support.
Speed of response required	Standard speed of response – would be supported by a centralised model. Where a high speed of response times is required (eg Crisis sites) – may require a more federated model supporting specific business processes.
HQ vs non HQ function	A large HQ will generally have a greater information requirement than smaller units, and is therefore likely to need a larger iHub function to support the user base.

REDACTING DOCUMENTS

Overview

1. Redaction is the removal of material in a document to allow the selective disclosure of information. Successful redaction creates a document that is suitable for release, even though the original document couldn't be disclosed in full for sensitivity reasons. Redaction often comes into play with Freedom of Information Requests.

2. It's important to get it right … there's no point in trying to redact a document (paper or electronic) if the recipient is able to see what you were trying to remove. Mistakes are made though, even in the MOD! So if you are involved with redacting a document, make sure you do it properly.

3. The National Archives have published a Redaction Toolkit – this is the authoritative document for all redaction work across Government. The lead department in the MOD is ISS Information Rights.

Why and when is redaction required?

4. Any document that contains sensitive or personal material should be redacted before giving it visibility to a wider audience or placing it in the public domain.

5. If you believe that a redacted copy of a document is required, contact your Information Manager or FOI Focal Point who should arrange for redaction or authorise you to carry it out on his behalf.

Points to remember about redaction

6. Redaction must always be carried out on copies, whether on paper or in electronic format, so that the original document remains unchanged.

7. Redaction must be secure – the end result should be that:

   a. the redacted material cannot be seen or the content guessed due to inadequate redaction;

   b. words cannot be made out when the physical document is held up to the light, and the word/material cannot be guessed because elements of letters at the top, bottom, left or right of the word are visible;

   c. changes in electronically redacted documents cannot be reversed.

8. You must be absolutely sure that redacted information cannot be recovered. Be aware that in hard copy, some marker pens do not completely obliterate text, and in soft copy many applications allow deleted and blanked out text to be recovered.

9. Where a large proportion of the document is to be redacted, producing a summary of the information may be a more viable option. A summary may also be a more secure option, eg in the case of regular reports that follow a standard format as the reader can draw conclusions from increased redactions year-on-year. However, in the case of legal proceedings, a summary is unlikely to suffice and a redacted copy of the relevant documents (with an explanation for the redactions, eg protectively marked information) may be required.

10. Further information about handling FOIA Requests For Information (RFIs), the application of the Public Interest Test, the calculation of redaction time in the Fees - Appropriate Limit, and processing of Subject Access Requests (SARs), is available on the Information Rights Intranet site.

What you need to do

11. Decide whether there is a requirement for a document to be redacted: is the information in the document needed in a releasable form, for example, in response to a FOIA RFI?

12. Consult the guidance to ensure that you understand redaction options. Decide whether physical or electronic redaction is appropriate, or if a summary is required.

13. Make certain that redacted information cannot be recovered – be particularly careful about metadata and tracked changes in MS Office documents. See How To Guide on ***Removing Hidden Data***, and The National Archives Redaction Toolkit 2011 (www).

14. Ensure that all information which should not be released is removed consistently throughout the document, especially where unique identifiers are used, eg a named person.

15. Keep a copy of the released document with a note explaining the reasons for redaction, and maintain a link with the original document. (This is particularly important in legal proceedings, when dealing with FOIA RFIs, and SARs in accordance with DPA98, where the applicant/data subject may appeal the decision to withhold information to the Information Commissioner.)

16. Where recurring documents are frequently required in redacted form, consider writing the document in sections, or with annexes, one of which contains the information which is normally redacted.

REVIEWING DOCUMENTS

Overview

1. This guide offers some suggestions on how to review and approve the documents you or your colleagues produce. Some MOD organisations have specific rules on how to staff papers – this just provides generic advice for writers and reviewers, and is not intended to contradict or override any local practices and procedures.

2. It is all too easy to produce documents of poor quality – ones that don't do what they're supposed to do, or don't serve any purpose at all. If your document can't be read and understood by the intended audience, then you've wasted your time in producing it, and you're going to waste the audience's time as well. Carrying out reviews will help you to produce work of the right quality.

When and how to review content

3. If in doubt, review – it will cut the number of mistakes, and improve the quality of your outputs. There are costs – time spent preparing, reviewing, negotiating and editing, for example – but these will almost certainly be outweighed by the benefits associated with producing a better product.

4. In general, don't publish documents of significance without some form of (documented) review process to assure fitness for purpose. Some won't need a full review but it is still good practice to get someone else to proofread them, as well as you, before you publish.

5. If you're responsible for the document, here are some ideas to consider:

- you need to decide how thorough the review process needs to be. Review documents to a level commensurate with their importance, and set the level of quality accordingly. You have to rely on your judgement, knowledge and experience here. To help make a decision, ask yourself these important questions, remembering that all of the people involved in the review will need to know the answers in due course:
  - what is the document for? Why is it being produced?
  - when does it need to be produced by?
  - who is going to read it? What are their expectations?
  - how important is the document?
  - what is the required level of quality? What constitutes fitness for purpose?
  - what is likely to happen if the document turns out not to be good enough?
  - who are the best people to review this?
- make sure the document is approved by the appropriate people (internal, and in some cases, external). By doing this, they certify that it is ready for issue and that it has, therefore, been reviewed enough;
- invite the right reviewers;
- if the document warrants it, issue a draft Product Description for Level One review;
- be realistic and courteous. Give reviewers some advance warning, where possible, and ample time to review the document and to prepare feedback;
- don't leave reviewers to resolve your conflicting or confusing review requirements – it is almost impossible to review any substantial document at several levels - structure, content, grammar and presentation – all at once. Think about simplifying the review process (see the diagram), by breaking it into three logical and distinct parts:
  - Level One (Structure) – review the proposed document structure (possibly in the form of a draft Product Description);
  - Level Two (Content) – review the content – the meaning, the message, the words, the tone and style;
  - Level Three (End Product Review) – check spelling, grammar, presentation, document status etc. It's a final consistency and accuracy check, nothing more;
- make it clear what you're asking people to review. Set realistic assessment criteria;
- after each review, determine the overall result, decide what needs to be done next, and make sure approval is given to move on. Here are four possible outcomes:
  - accept the product at this level of review, because no changes are required;

- accept the product at this level of review, subject to agreed changes being made and approved;
- schedule another review at this level – after more work;
- schedule review at an earlier level;

- keep an accurate record of all Review and Approval steps and activities - feedback received, changes made etc;
- reviews (especially Content ones) may need to be repeated one or more times until you are happy that the relevant acceptance criteria have been met;
- if you decide not to accept individual review comments, try to explain and record the reasons why. If necessary, talk to the reviewer about any issues you have. If you can't reach agreement you, as the person responsible for producing the document, can overrule them, but rememberit's your risk now;
- approve key documents after review and before issue, and retain evidence of these activities;
- when the review step is complete, make sure that you amend the document's issue status by changing the document issue number, release history and footers;
- make sure the status of the document is clear and your version control is adequate. For example, if the document status is Draft for Comment, then show this on the document somewhere.

6. Here are some useful ideas for you to consider, if you've been asked to review something:

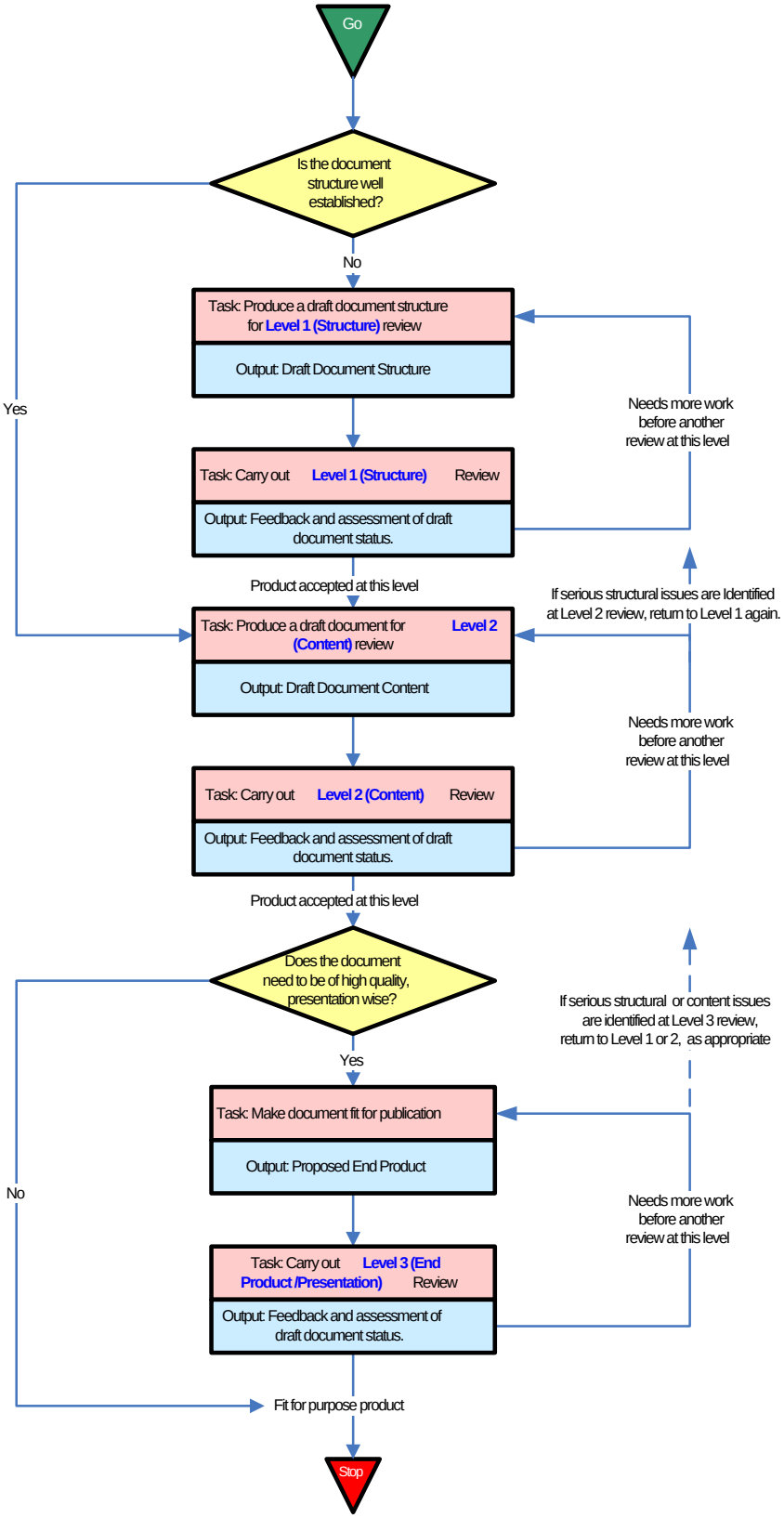
- be thorough, courteous and professional. Get the tone of your response right. Give useful, considered feedback;
- is there an existing Product Description? If there is, use it as a guide;
- check if there are any relevant quality standards. If so, make sure they are met;
- offer feedback in a format acceptable to the document owner or author.

Reviewing as a Development Activity

7. Both author and reviewer benefit considerably from the review process, not just in learning more about the subject in hand, but also in improving styles of writing. Accurate, brief, clear communication is critical to Defence business, and by reviewing other people's work, and having our own work reviewed by others, we are likely to improve our own ability to write quickly and effectively.

Suggested Outline Process (Complex Document)

8. Suggested Outline Process (Complex Document) Below is a suggested process for a fairly complex document, likely to be widely read, where it is important to get it right.


Go
Is the document structure well established?
No
Yes
Task: Produce a draft document structure for Level 1 (Structure) review
Output: Draft Document Structure
Needs more work before another review at this level
Task: Carry out Level 1 (Structure) Review
Output: Feedback and assessment of draft document status.
Product accepted at this level
If serious structural issues are Identified at Level 2 review, return to Level 1 again.
Task: Produce a draft document for Level 2 (Content) review
Output: Draft Document Content
Needs more work before another review at this level
Task: Carry out Level 2 (Content) Review
Output: Feedback and assessment of draft document status.
Product accepted at this level
Does the document need to be of high quality, presentation wise?
If serious structural or content issues are identified at Level 3 review, return to Level 1 or 2, as appropriate
Yes
Task: Make document fit for publication
Output: Proposed End Product
No
Needs more work before another review at this level
Task: Carry out Level 3 (End Product /Presentation) Review
Output: Feedback and assessment of draft document status.
Fit for purpose product
Stop

.

EFFECTIVE WRITING

Overview

1. Good written communication is vital to the work of Defence. Clear writing reflects clear thinking. Simplicity, accuracy and brevity matter. We very rarely need perfection, but always ask yourself whether what you've written is good enough for its purpose.

2. Sometimes what we write will be read by people who were not the original target audience, perhaps even into the public domain. This may for example be through an FOI request, or evidence at an Inquiry - it may even find its way into The National Archives as a public record. If your name is on it, you will want it to show you as a real professional in your work for Defence.

3. JSP 101, the Defence Writing Guide, sets out the conventions of Defence Writing, and provides basic document formats.

4. Below is some general advice on effective writing in Defence. Experienced writers will probably do most of this without thinking. There are of course a lucky few with a rich talent for writing, who can break all the standard conventions, and their output is still brilliant. However, for the rest of us, these tips might help.

Handy hints and tips

5. We don't always need to write … sometimes we can just talk to each other! So write if:

- your message is too detailed or complex to deliver verbally or it may need to be studied carefully;
- information has to be conveyed to a wide audience;
- you need to keep a record.

6. Before you begin writing:

- always give yourself time to prepare.

7. Focus on what really matters:

- know why you are writing and think about what you're going to write;
- be clear about the scope;
- know who your audience is. Will they be familiar with the subject?
- think about the style and tone you're going to adopt. What is going to suit the audience?
- are you writing on behalf of someone else? If so, adjust the style accordingly;
- for longer documents, get the structure right, using this as a basic template:
  - Introduction (tell them what you're going to tell them) - summarize background information and say why you are writing, as concisely as possible (preferably in one paragraph);
  - Main Body (tell them) – here, in as many paragraphs as necessary, present facts and list any arguments or problems logically, highlighting any key points;
  - Conclusion/Summary (tell them what you told them) – here, highlight any required follow-up action and, where necessary, summarize key points;
- choose the most appropriate layout and look;
- select the most appropriate channel medium;
- what level of quality is required? (Very high if you're writing for a Minister).

8. Try to make your writing:

- accurate, concise, clear, simple, and relevant;
- reasoned and logical;
- polite and respectful, and (where appropriate) personal and friendly.

9. When writing letters on behalf of the MOD, that are personal to the recipient, we need to be careful to adopt a natural style, and not sound bureaucratic. Remember to include your signature block and contact details too.

10. Here are some general tips:

- use an approved document template, if one is available;

- use a reputable dictionary to check on the meaning of those words that you don't use regularly – it's much safer than guessing.
- use your spell-checker, but remember it checks for spelling, not that you've used the right word (we've all seen 'manger' when the author meant 'manager');
- use Plain English, so that your audience will clearly understand you;
- stick to one main subject in a document;
- keep the number of abbreviations (including acronyms) to a minimum. Unless you're absolutely sure they will be understood, make sure you explain them on first use;
- only include diagrams if they're going to improve things;
- avoid gimmicks – for example, overuse of text highlights, can hinder clarity;
- avoid the temptation to over-engineer your writing – we are aiming at fitness for purpose, not a literary prize;
- when writing on your own behalf, use the first person singular, as this will allow you to express strong opinions, but show that they are personal views, rather than corporate ones. When writing for someone else, adjust your writing accordingly;
- keep to the subject;
- use simple, short words and phrases;
- use the most appropriate document format;
- use paragraphs and lists to break up your writing and to provide a clear structure;
- be clear. Include only one main point in a sentence and only one or two points in each paragraph. Deal with them fully;
- review, approve and publish all written material, irrespective of format, prior to release, in line with all relevant (local) quality, configuration and change control standards and procedures;
- when writing letters on behalf of the MOD, that are personal to the recipient, adopt a natural style, and don't sound bureaucratic.

11. Before you send it, imagine yourself as the recipient, and read it carefully. Has the document conveyed the right message in a professional way? Remember to include your signature block and contact details too.

Some useful reference sites

12. These may be useful:

- Plain English Campaign (try their Gobbledygook generator)
- BBC News Style Guide, Telegraph Style Book, Guardian and Observer Style Guide, The Economist Style Guide;
- GOV.UK website style guide.

GETTING THE BEST VALUE FROM MEETINGS

Overview

1. Meetings can be an effective and efficient way of exchanging information, understanding other people's viewpoints, and reaching agreements. Effective meetings build enthusiasm and commitment for the shared goal, resolve differences, highlight problem areas, allocate tasks, and make decisions. It is hard to match the efficiency of a well-run meeting to resolve complex issues by any other means.

2. However, meetings are expensive in time and money, and often regarded by attendees as an unproductive use of time - sometimes, you will come away wondering why you and others were invited to attend or why the meeting took place all.

Is a meeting necessary?

3. Decide the aims of the proposed meeting, and ensure that a meeting is the appropriate vehicle for accomplishing them. Consider the cost of time and travel, and possible alternatives to a formal meeting. If the same objectives can be met through, for example, a conference call by phone or video, an online discussion, update of documentation on a team site, or one-to-one discussions, then it is probably quicker and cheaper to use one of these other methods.

Planning the Meeting (Chairman/Secretary)

4. Establish an effective meeting plan and determine the focus, agenda, and participants. Decide who should attend, and check availability. If a delegate attends in the place of a crucial decision maker, make sure they have the authority to make decisions. Postpone the meeting rather than hold it without critical members.

5. If this meeting is a sequel to a previous meeting, check the status of actions agreed at last meeting.

6. Distribute the agenda and preparatory work in good time. Provide reading material in good time to provide participants with opportunity to consider implications and obtain necessary facts. Thorough and comprehensive material should engender commitment and confidence from attendees. As always, be realistic in the volume of material provided, and don't burden others excessively.

7. Decide whether proceedings are to be recorded in full minutes, or as a brief record of decisions.

8. If you want to make a voice or video recording of a meeting, ensure you gain the consent of **all** the attendees before you start recording. Use only MOD devices to make any recording, and make a transcript if you wish. Once you have issued a record of the meeting, it is probably best to destroy the recording and any transcript (but if it's important to keep it, manage it properly through your unit).

At the Meeting (Chairman)

9. An effective Chairman, who keeps participants on track, ensures the accomplishment of the desired results from the meeting. The Chairman should:

- set a positive, productive tone for interaction among the participants;
- ensure participants know who each other are, and whom they represent;
- start the meeting with a review of the goals or anticipated outcomes and the agenda;
- review minutes and actions from previous meeting;
- involve all participants relevant to the subject matter, not just the more vociferous;
- use the preparatory work distributed before the meeting;
- ensure that sufficient time is allocated to certain discussion points and aim to keep the meeting on track – timing is crucial;
- conclude each agenda item with statement of actions (what must be done, by whom, and when), ensuring they are realistic objectives;
- help participants stay focused and productive;
- have fall-back plans should discussion points require additional time; these may include cutting short some of the other points which may be considered of lesser importance or scheduling another meeting if required.

Closing the Meeting (Chairman)

10. The Chairman should:

- summarise action points;
- determine if need for further meeting, and if so, when;
- consider a formal debrief of Meeting, inviting participants to comment on effectiveness of meeting and progress they feel the group is making on the topic of the meeting. Future meetings should reflect the evaluation.

After the Meeting (Chairman/Secretary)

11. The Secretary should produce the minutes (or record of decisions) as soon as possible - preferably within a day or two of the event. The Defence Writing Guide has advice.

12. The Chairman should then review the draft minutes, and if content, give approval for them to be published;

13. The Secretary must then publish the minutes or record of decisions, making sure that a copy is retained in the appropriate place within an approved record management system;

Between Meetings

14. The Chair and Secretary should, from time to time, check on the progress of the various tasks and actions agreed during the meeting, and take steps to hasten them where necessary.

Advice for participants

15. All participants should:

- prepare for meetings thoroughly;
- arrive punctually;
- keep focused during the meeting, and help the Chairman and Secretary achieve their goals;
- fulfil actions allocated, keeping the Chairman and Secretary informed.

Conference calls – audio, video, online

16. These can save a lot of time and cost. The principles are all the same as any other meeting. Allow some extra preparation time for video, to ensure the technology, lighting, acoustics and visibility are all fine, and that there are no background distractions that deflect from purpose of meeting.

USING STORAGE AND BANDWIDTH EFFICIENTLY

Overview

1. Although computer storage and communications costs are continually dropping, it's still important that we use these resources efficiently; failure to do this can incur significant extra costs for MOD. Also, as servers fill up and communication links become overloaded, we are more likely to experience poor performance and reliability. There is also the risk of breaking the law if personal information is held longer than necessary.

Advice on using storage and bandwidth more efficiently

2. Here are several pointers to help you to use less storage and bandwidth. You should:

- **store a single copy of information in the appropriate shared area**, instead of each member of the team storing their own copy. As well as saving storage, this is good Information Management practice, and ensures everyone has easy access to the latest authoritative information. This is particularly important with large documents such as image, video and audio files;

- **create and maintain unit–wide presentation galleries**. PowerPoint presentations are often stored many times, and are often very large, particularly where photographs and video clips are included, so it makes sense for units to create their own presentation gallery or galleries (available to the entire unit, and beyond, as necessary) to hold master copies. This not only saves space, but also helps people who are preparing new presentations to see what's already been produced. Ideally reference slides would be created and kept up to date; staff could then pick from these to create slide decks quickly and easily for a particular audience. But failing this they can at least reuse or adapt old presentational material if they need to, rather than starting afresh – a big advantage;

- **keep emails short, simple, and to the point**. Also make good use of instant messaging rather than email for the trivial;

- **send emails and meeting requests with links, not attachments, wherever possible** - put information of significance in documents stored in appropriate shared areas, and send links instead. This is easy to do, and it keeps email sizes down – your colleagues won't need to waste their email filestore retaining the attachment(s) you've sent them. However, there are a few exceptions. You should send an attachment rather than a link when sending a file:

  - to people who are not on the same network as you, and who, as a result, are unable to access the shared area where the file is stored;

  - to people who may not have permission to access the shared areas containing the document;

  - where it is essential that the addressees receive the document exactly as you sent it. Unless the document is stored in an electronic records system, or other repository where it cannot be amended, you may need to send an attachment;

- **avoid cascading emails** - in general, communicating information using an email cascade is inefficient, both for the people involved, and for storage and bandwidth resources. It is also slow and liable to delay, and often fails to reach all the intended recipients;

- **never send emails to large numbers of addressees** where it is possible to publish the information to the Intranet or a local shared drive or team site. Ideally recipients would have Alerts configured, otherwise you may need to send them an email to alert them to the newly published content;

- **minimise the size of content** which you create or import: the two biggest issues are emails because we send so many of them, and documents containing images, video, audio or diagrams because these can take up large amounts of storage. Consider:

  - creating emails in Rich Text instead of HTML format, which makes the emails significantly smaller;

  - creating images and other large content types in the most suitable format. JPEG is usually the most efficient form of image file, so storing images (or adding them to documents) in this format can produce big savings on storage. However this can vary depending on the style of the image, so it may be worth checking the size of your image in various formats;

- **clear out files and folders** to remove documents that are no longer needed: a significant proportion of the material on MOD systems is no longer relevant, either for current use or as a record of previous activity. Key areas to concentrate on are:

  - recycle bins. Some MOD systems, including DII(F) do not empty recycle bins automatically. You need to access the recycle bin (usually from desktop), and delete the content;

  - calendar entries. It can be useful to keep some history in your calendar, but many of the entries have no long term value, and can be cleared out. In particular, find those calendar entries that contain large attachments (such as presentations) – these attachments should either be moved to the right shared area, or deleted (and if you get calendar entries with attachments, ask the organiser to send links in future, as advised above);

  - old folders and team sites containing legacy documents that are unlikely to be needed;

  - large files (find these by sorting or filtering), in particular graphics, image, video and audio files. You might find irrelevant material … you might even find material such as commercial music files held in breach of copyright (which would be illegal – delete!);

  - unnecessary duplicates. Duplicates should only be retained where context is important (for example to demonstrate that a particular unit did have a copy of an operational order at a point in time). Identifying duplicates can be difficult and time consuming. In the absence of specialist tools the simplest method is to search for the name of a file to identify duplicates, though this method is not 100% accurate;

  - personal information (in particular relating to other people, such as draft staff reports or similar) that is no longer required. This is not just a matter of computer storage – this is about complying with the Data Protection Act.

- **keep what is important, and store it correctly** - ensure that significant information is retained in a properly managed shared area. If in doubt, ask your colleagues in the iHub.

Points specific to Microsoft Environments

3. Most of use Microsoft software and there are some bad practices we should avoid. Therefore:

- **do not create .pst (personal storage) files for Outlook** – there are a number of reasons for this, including difficulty of search and retrieval … so don't do it;

- **avoid using My Documents as an archiving tool** – with the exception of personal documents, your My Documents folder should contain only early drafts of items which you are working on. When you have finished with them, move them into shared areas and delete them from your personal storage.

Additional points specific to DII(F)

4. DII(F) has two mailboxes (for all except occasional users) – role and personal. If there are messages in the mailbox which the sender has marked Private, and these are in your personal mailbox, you will not be able to see them if you access Outlook with your role profile (which is what people usually do) – this applies even if you have sent the messages yourself, and ticked the message option box marked "private". It is very important that you periodically open Outlook with your personal profile, and clear out any documents that you should no longer be holding (eg civilian PARs relating to previous years). Remember that if you retain personal information longer than is necessary, you are in breach of the Data Protection Act.

5. The amount of material held in the DII(F) mailboxes should be small. Rarely should it be necessary to retain messages – if the information is important, it should generally be in a shared area; and if it's not important enough for that, it's unlikely to be worth keeping at all. Basically all that should be found in mailboxes is:

- recently received material, that has not yet been dealt with, or which is of short term value only;

- calendar entries (current and future, and where still relevant, past);

- personal information related to MOD employment, unsuitable for shared areas.

6. The same principles apply to the My Documents area. Other than personal information, the only material that is likely to be needed there is very temporary – for example, the first draft of a document too

immature to be put in a shared area, and which would be of no value to your colleagues if you were away and unable to work on it.

7. Because of the varying natures of people's jobs, the number and size of messages they receive, etc, it is hard to be prescriptive about the physical amount of material that they should have in their mailboxes and My Documents. It is also true that large mailboxes are often not the fault of the individual, but rather reflect the fact that far too much material is being sent around their organisation in the form of emails, rather than being put in shared areas.

8. In order to ensure that material that should be in shared areas (or which shouldn't be on MOD systems at all) is not being held in individual mailboxes or My Docs, Units are expected to monitor the sizes of these individual storage areas – if your Mailbox or My Documents size exceeds these reasonable sizes, you will be probably be asked for justification.

Additional guidance for people in IM specialist roles

9. To improve use of storage and bandwidth in your unit, you should:

- **help your colleagues understand why this is important** - people will be used to having almost unlimited storage and bandwidth on domestic computers, and may find it difficult to understand why they are so constrained here. Part of the answer is to do with costs of a managed service, and the demands of the operational space; the other part of the answer is of course making sure that all significant information is properly managed at unit level, available to the right people and protected from the wrong ones, and retained as appropriate;

- **make sure you have an effective monitoring regime in place** - a range of techniques may be necessary, including:

  - checking usage of personal storage areas, to make sure they are being used in moderation;
  - ensuring that shared areas are being properly populated with the right material; and
  - giving advice when attachments are being used instead of links;

- **help people to understand where to store information, and where to find it**. Create file plans that people can, and do, understand – that are simple, straightforward, logical and intuitive. Publicise them and then make sure people use them.
- **ensure people are given high quality training and support** - include advice on where to find the right documentation, so people can help themselves;
- **look out for inactive, orphaned, irrelevant and un-owned libraries and folders** - if you find one, do some research to check if it's still needed (as a record, for example), and if it isn't, delete it;
- **use statistics to help you**: if you have tools capable of identifying what is stored where, how large folders and files are, whether you have duplicates, etc, make full use of them – it's a lot easier than doing things manually;
- **monitor storage used in individual Mailboxes and My Documents** - there may be very good reasons why people are using a lot of Mailbox and My Documents storage, but you need to know what these are. In particular you should guard against:

  - material being held in individual areas because it is seen as quicker and easier (ensure people know where they should be storing material, and why);
  - material being held that should not be in MOD systems at all, eg commercial music held in breach of copyright, old staff reports on others that should have been deleted after upload to HRMS/JPA, photographs of social events;

- **ensure that Commanders lead by example** - this is by far the quickest and easiest way of embedding good Information Management practices within your unit. Persuade the Commanding Officer / Head of Unit to insist on receiving links to documents (not attachments or lengthy emails). Encourage them to instruct all members of their team to store all significant material in shared storage (in the right folder of course).

USING THE ENTERPRISE GATEWAY SERVICE

Enterprise Gateway Service

1. The Enterprise Gateway Service (EGS) provides a link between MOD networks and the Internet, for access to web sites and transmission of emails.

2. The service includes web filtering software, which groups websites according to category. MOD decides which categories of web sites should be accessible to users, and which should be blocked. This guide explains why some sites are blocked, and what procedures are to be followed if you find sites which are blocked, when they should be allowed.

MOD Web Site Filtering Policy

3. MOD's policy is that access to the Internet should be fairly open. We aim to allow access to all web site categories, and individual web sites, except where such access is likely to:

a. contravene the MOD Acceptable Use Policy (JSP 740). We therefore block:

- categories such as gambling and pornography;
- individual sites such as commercial auction sites;

b. pose a risk to the technical security of the network, or to broader information security. We therefore block:

- categories such as web-based mail systems and translation sites;
- individual sites such as those using mobile code, such as Java or Active X;

c. result in excessive consumption of bandwidth or other resource. We therefore currently block

- categories such as streaming media and social networking sites.

Implications of Filtering

4. MOD does not allow individual sites within a blocked category.

5. If you find that a particular web site that you need is blocked it is unlikely that it will be made available, but you can contact the BT CASC (Customer Assured Service Centre) who should be able to explain why it is blocked. If this does not resolve your issue, BT CASC will refer queries to ISS Ops. However, the quickest way to access a site blocked by EGS will almost invariably be to use a device with direct access to the Internet.

6. Although MOD invests heavily in filtering software (and protection against spam), it will never be possible to filter out all inappropriate sites and block all spam. This is a risk that must be accepted if you have an EGS account (or access the Internet in any other way). If you find a website that you believe should have been blocked, but hasn't, contact the BT CASC.

DEALING WITH SPAM

Overview

1. Spam is the name given to unsolicited or unwanted email or text messages sent to people, often in the hope that some of these addressees will respond. Much of it is commercial advertising designed to promote products, but it can take many other forms. A spammer can send out millions of messages in a day, and will probably only need a few responses to achieve their targets.

2. Spam is a nuisance – it clutters Inboxes, it annoys, it offends, it leads to fraud, and it's a threat to networks. The first line of defence is to avoid your contact details (email address, mobile number) falling into the wrong hands in the first place, but that can't be guaranteed. The Enterprise Gateway Service (EGS) – the link between our internal networks and the Internet – blocks the vast majority of spam emails, but it's impossible to stop them all (without stopping some perfectly legitimate emails as well).

What to do (and what not to do)

3. Report spam to the SPOC, using email address SPOC-Spam, and following their instructions.

4. Don't respond to spam. It is possible that the return address is invalid anyway, but it could turn out to be someone else's address, and sending a response will make you into an unwitting spammer. If the return e-mail address is genuine, you'll have instantly verified that your e-mail address is active, and your details will just as likely be sold to other spammers. Don't be fooled by requests such as "**click here to unsubscribe**". Don't follow the instructions – delete the email. It may look as if you've been given the chance to opt out of receiving further spam, but it is more likely that the spammer is looking for evidence that your e-mail address is still active.

5. Don't send or forward spam emails to other people, unless you've been asked to do for good reason. The MOD's Acceptable Use Policy bans all unauthorised onward transmission of spam.

6. Don't give your contact details to all and sundry. You risk having your email address added to a distribution list over which you have no control. Be careful when recording your email address or addresses on a web site or forum, and only subscribe to ones you trust.

7. Don't click on any link in an email (including suspected spam) if you're not sure of the source. Some emails are made to look like official emails, with the actual address of the link disguised.

8. Don't open any attachments to an email unless you're confident in their source.

9. Don't use your MOD e-mail address to sign up for anything unless you're sure of the site's reliability. Once in the spammer's databases you have no way of getting it out.

10. Don't forward Chain Letters or hoax email, unless you have been told to do so with good reason. Otherwise you'll breach the MOD's Acceptable Use Policy (AUP).

Improving your knowledge

11. Keep up to date with MOD guidance. The MOD Cyber Skills team publish articles and provide expert advice.

12. Take a look at "Get Safe Online" - this is a website sponsored jointly by HM Government and Industry. It provides practical advice on how to protect yourself, your computers and mobile devices against fraud, identity theft, viruses etc. It even covers safe online gaming and dating (though you mustn't do either of those from MOD computers … it's against the AUP).

PROTECTING PERSONAL INFORMATION

Overview

1. Losing personal information or allowing it to fall into the wrong hands is not a good thing to do. There have been many high profile incidents in the UK and elsewhere. Some have involved those of us working in Defence. It can happen anywhere – at work, at home, at play – and it's not just confined to negligent use of IT equipment. The same basic rules apply whenever you deal with personal information, irrespective of format, medium or location.

2. It's a behavioural and cultural issue more than a technological one, although technology can allow us to lose huge volumes of data very quickly. It doesn't matter if you're using a computer, a phone, writing a letter or chatting with friends. When you handle personal information (yours and others), it becomes your responsibility to protect it, so take extra care and stick to proven, good practice.

Making a start

3. A good way to start is to think about your attitudes towards personal information, and the way you manage and use it. Are you careful enough? Do you know:

- why you should protect it?
- what, by law, you're required to do?
- what you need to protect?
- when you should be at your most vigilant?
- how to protect it?

4. You need to keep personal information – yours and others – as private and secure as it needs to be, to help prevent, amongst other things:

- identity theft;
- risks to personal safety;
- financial loss;
- fraud and illegal trading;
- invasion of privacy.

What does the law say?

5. The Data Protection Act tells you what, by law, you're required to do, wherever you are and whatever you're doing. Personal information must be:

- processed fairly and lawfully;
- obtained for specified, lawful purposes, and then only used in ways compatible with them;
- adequate, relevant and not excessive;
- accurate and up to date;
- only kept for as long as necessary;
- processed without infringing your rights;
- protected and secure;
- not transferred to other countries without adequate protection.

What do you need to protect?

6. Protect the things you use to record or store personal information – computers, mobile phones, notebooks, paper files, address books, diaries, etc – wherever they are. If it's your own personal computer, this means keeping things such as the operating system, anti-virus software, anti-spyware software, firewall protection and data encryption facilities up to date.

7. Think about the information you're dealing with. Is it, for example:

- basic personal identification information – for example, name, home address, home email address, personal telephone numbers, date of birth, height, weight, photographs, signatures (or copies of);
- anything to do with personal finances, including credit/debit/store card details and receipts, cheque books, bank statements, payslips, account details, and finance related correspondence and information;

- personal medical information;
- information about a person's work - staff/service number, vetting details, work address etc;
- information about a person's private life, lifestyle or social activities;
- things which, if lost, could compromise security of, say, a bank account, computer logon etc – including, for example, Personal Identification Numbers (PINs) and passwords.

When to be cautious

8. Be careful at all times, but be extra vigilant when:

- shopping, banking and making payments online;
- booking holidays and travel;
- communicating and corresponding – when sending emails or letters, using social networks, (including message boards and chat rooms), blogging or contributing to wikis;
- letting your children go on line;
- you're asked to provide personal information (yours or others) – and not just when on line;
- involved in on line auctions;
- paying by debit card, credit card or other charge cards;
- using a cash machine/ATM;
- dating on line;
- playing computer games;
- sharing files;
- filling in forms;
- dealing with people you don't know. Be as careful when on line as you would when meeting in person;
- using computers that are not your own;
- you're using IT or have finished using it – secure it, lock it up, switch it off.

How to Protect Personal Information

9. Some hints and tips:

- think about personal information as you would do official secrets. When you're dealing with it, it becomes your responsibility. Stay vigilant and think before you act.
- get to know the law a little bit more;
- when people ask you for personal information (for example, over the Internet or over the phone), be wary. Challenge them to justify why they need it, especially if they work for the MOD. You don't have a duty to share it with them. Only provide the information that is justifiably required for the reason specified. Only do so if you've certain you know who you're dealing with. If in doubt, seek advice. Think about the potential consequences of your actions, and make every effort to not let personal information fall into the wrong hands;
- be careful not to give the wrong people too much information about where you are. It's easy to do this without even knowing, especially with modern social media;
- protect the IT equipment you carry around with you. Make sure the equipment is security tagged or marked in some way. Keep a record of it. Don't advertise the IT you're carrying – hide items in protective bags, disguising the contents;
- when using the postal service to send personal information, use the most secure option available;
- sign new credit cards, debit cards and store cards as soon as you receive them;
- destroy items containing personal information when they are no longer required – for example, cut up SIM/bank/store cards and destroy hard drives of personal computers;
- before passing on or disposing of electronic mobile devices (eg mobile phones, personal digital assistants, smart phones etc.), make sure that you delete all of the personal information stored on them;
- shred old documents;
- check statements regularly – bank, credit card, utility bills, for example;

- make backups. look after them, keeping them as secure as they need to be;
- use trusted methods of paying for things (on line or elsewhere);
- be careful what you respond to. Don't open suspicious emails, or email attachments. Beware of spam. When on the web, look out for suspicious websites. Don't open them. If in doubt, leave them alone – ask yourself, are they legitimate? Can you trust them?
- select PINs and passwords with care, avoiding ones other people will be able to guess. Look after them. Don't share them with other people;
- run a personal credit report check from time to time;
- block unwanted mail/telephone calls;
- when moving house, tell banks, utilities, friends as soon as you can, and get your mail redirected;
- wherever you are – at home or at work – question the way people handle information, and suggest ways of improving them and making them more robust;
- limit the number of people with access to personal information;
- don't display your MOD security pass when you're outside MOD premises;
- track all copies in whatever form at the proportionate level of security;
- if you've logged on to a computer, but need to leave it unattended – lock it;
- don't use scanned signatures;
- don't install software or programs you're not sure of, whatever computer facilities you're using;
- stay alert to potential scams and hoaxes;
- keep yourself up-to-date on information protection issues and news;
- be careful when using social networking facilities:
  - use the privacy tools they offer. Set up the protection you need before you begin to use the networking site, and keep all of your security software facilities up to date;
  - read and abide by the acceptable use/privacy policies of the site you're using, if they exist;
  - proceed with caution. Be careful about the personal information you provide and the opinions you express on-line - once the information is out there, you lose control of it;
  - find out who you're dealing with.

Improving your knowledge

10. There is excellent advice at Get Safe Online, including a whole set of pages dedicated to Protecting Yourself, covering such topics as Preventing Identity Theft, Cyberstalking, and Webcam Blackmail.

USING A WIKI

About wikis

1. A wiki is a way of group working: a website where people can add, edit or remove content from a page, and where all previous states are retained for reference. Wikis make it easy for contributors to develop content and to capture, develop and share ideas, information and knowledge quickly. Wikis characteristically use only a standard browser interface, make creating and linking pages intuitive and allowing people to contribute with the minimum of fuss.

2. Wikis are useful for people in expert communities, but they can also work for wider communities too – though the people managing the work need to understand that errors and inappropriate content (whether intentional or otherwise) may well be introduced along the way.

3. **Advantages** – wikis:

- allow ideas to be recorded quickly, allowing more time for editing and producing formal documents;
- enable instant collaboration, without the use of email (or similar) to keep people informed;
- allow anyone with a browser, and permissions to the site, to access the material and contribute; and
- retain a comprehensive archive, with each revision being stored automatically.

4. **Disadvantages** – wikis often:

- require careful moderation: open editing can trigger battles over content or worse – vandalism, for example, which need to be corrected as soon as possible;
- show dirty laundry in public: a wiki is a group memory, displaying partially formed and speculative ideas, and is often untidy – so be aware of this before making a wiki public;
- become messier (and unusable) over time unless they're managed properly;
- offer only limited and feeble formatting, so it's likely that you'll have to transfer the content to another document type, and reformat it there – all extra work; and
- intimidate the less technically capable – people have to be able to mark up text and find their way around a constantly changing site.

When should you use a wiki?

5. Think about using a wiki to help develop document content. At some point you'll need to freeze the content and then copy it to another format, so that you're able to produce a polished end product ready for publication. Don't use a wiki as an authoritative document – because they're easy to change, errors, inaccurate information or inappropriate material can creep in.

How should you manage a wiki?

6. Managing – setting up, maintaining, monitoring - a wiki takes time and effort, but it's important to do it well, so that you get the most out of the wiki, keeping threats at bay and dealing with problems before they get out of hand.

7. If you're setting up a wiki:

- be clear about the scope of the work;
- make sure you're confident that benefits will outweigh costs (time, commitment, etc);
- check there isn't a group somewhere already addressing the same issue;
- familiarise yourself with the tool(s) you're planning to use;
- host it on the appropriate facilities, making sure that all of the people you want to involve can access and use it; and
- recruit a skilled moderator to steer the work and monitor people's behaviour;

8. If you're a moderator of a wiki:

- allocate time to task;

- manage it in line with relevant rules (as a website hosted on a MOD network); and
- monitor its contents to make sure that it's accurate and appropriate.

Who should be given access to a wiki?

9. It's an important question, but one without a definitive answer. It's often easier to only make a wiki available to a select few directly involved in the work, extending membership to others who express an interest as the wiki develops, rather than inviting many people to contribute and then (potentially) finding yourself overwhelmed by content - not all of it good quality. Ultimately, it's a judgement call.

STORING AND FINDING INFORMATION ON DII

Overview

1. This guide lists the main places where you can store and find information when using DII. It covers the Official (formerly Restricted) environment (although many of the same basic principles apply to DII Secret). It also gives advice on the types of information you should be storing (and, where applicable, publishing) in these storage areas. A summary is at the Annex.

2. The guide deals with unstructured information (documents, spreadsheets, presentations, etc.) rather than structured information stored in databases. It also can't cover every possible circumstance – it is more about helping people make the right decisions after thinking about the key issues (in particular, who should be able to access it (and who shouldn't), and whether it needs to be preserved as a Defence record.

Background

3. Across Defence, we need our information to be:

- reliable;
- legally held;
- labelled properly;
- stored in the right place;
- published via the appropriate communications channels;
- available to those people who should have access to it;
- protected from those people who shouldn't have access to it; and
- preserved for the appropriate period of time.

4. There are several types of locations where information can be stored, published and found. When storing, it is important to use the most appropriate location – in particular we need to think about the target audience (who we want to see it, and who we need to protect it from), and whether the information needs to be preserved as a record of business. The available locations include:

a. **Shared areas** (generally one or more of these will be the appropriate location)

- The World Wide Web (Internet);
- Defence Collaboration Programme (DCP) sites (for use with external organisations, in particular Industry);
- The Defence Intranet (DI);
- Meridio Electronic Records Management System;
- SharePoint Team Sites, Document Libraries and Site Extenders (SharePoint 2007 also called MOSS);
- Windows NTFS Shared Storage;
- Defence Gateway services.

b. **Non-Shared areas** (generally not an appropriate location for storage … transitory only)

- Microsoft Outlook;
- My Documents (Role and Personal folders);
- Off line storage (DVDs, CDs, etc);
- MOD Laptops.

The World Wide Web

5. The World Wide Web is an invaluable source of business information. Most business-related sites can be accessed from DII via the Enterprise Gateway Service (EGS), but there are restrictions to meet information or network security requirements.

6. The main MOD website, and the Service sites (RN, Army and RAF), are the appropriate places to store unclassified information that we wish to make freely available to a global audience. Typical examples will include News, Careers information, Policy documents, Statistics, information about structures and units, and published reports. These sites are controlled by Director Defence Communications (DDC). Publishing on the Defence websites is subject to strict control, to ensure quality and consistency. For more information, see JSP 745, and refer to DDC.

7. Note that material published on official world wide web sites must also be retained within the appropriate Records Management system (Meridio or NTFS as appropriate).

Defence Collaboration Programme sites

8. When working with partners outside MOD, a secure collaboration site accessible to the parties concerned may well be appropriate.

The Defence Intranet

9. The Defence Intranet (DI) is where authoritative information, relevant to a significant portion of the Defence community and carrying no significant restrictions on who can (and cannot) access it within Defence, should be published. Information published to the Defence Intranet is available to all DII users (ie Standard and Occasional) as well as users of other authorised RLI-based systems. This therefore overcomes the access limitations presented by both Meridio ERMS and SharePoint Team Sites (see below sections). Examples of the types of material that should be stored here include:

- Authoritative Defence policies, rules and guidance material (examples of publications involved here include Joint Service Publications (JSPs), Defence Instructions and Notices (DINs), Joint Doctrine Publications, Competence Frameworks, but there are many more besides);
- Defence news alerts and announcements;
- Operational information (as long as it is within the Official classification and can safely be made available across Defence), such as
  - Pre deployment information;
  - Reports, latest information and lessons learnt from theatre;
  - Tactical doctrine;
  - Operational training information;
- Internal web presences for Defence programmes, projects, initiatives, applications/tools, units, locations, associations, clubs etc;
  - This should be an overview of what your unit or team does, together with links to other pages or documents (related organisations and teams, key people's Enterprise Directory page, and, of course, the Team Site).
  - The Intranet page will be open to all Defence staff with access to DII (and some other systems on the RLI). Therefore do not include anything on the Defence Intranet that needs to be restricted to a subset of the overall user community. However, if you do want to attract people to your Team Site, ensure that your links from the Intranet go to pages that are open to your target audience.
- Reference Documents;
- Defence Journals, Magazines and Newsletters;
- Links to Applications and Tools;
- The Defence Framework (How Defence Works).

10. Publishing to the Defence Intranet is straightforward for those people with the appropriate publisher privileges, and the associated training (details provided on the Defence Intranet itself). Typically a unit will need several publishers, just to ensure that there will be always be someone available to publish new and revised material.

11. DI pages must be kept current – content, names, links, etc., will all need regular review and probably update. In particular, the feedback link on each page must be maintained, and monitored, by the page owner.

12. Note that significant material published on the Defence Intranet must also be retained within the appropriate Records Management system (Meridio or NTFS as appropriate); the Defence Intranet is a facility to allow users across Defence to access authoritative information and is not intended to replace Records Management or file storage areas.

Meridio Electronic Records Management System

13. 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 all units to determine what information has corporate value, and to make sure that this is retained. The purpose of an Electronic Records Management System (ERMS) is to ensure that, once stored, a record is not amended or deleted (by accident or design), thus helping to maintain a trusted record of business. These records should then be formally reviewed (and, where necessary, disposed of) according to a pre-defined retention schedule, and .

14. All items that your unit publishes on official Defence Internet sites or the Defence Intranet must also be stored in an approved records management system, because the MOD needs to keep an accurate record of what it publishes. Our official Internet sites and the DI are merely publication channels, not records management facilities.

15. Meridio is the ERMS product available on DII. Access privileges can be set on Meridio folders, similar to Windows NTFS folders, so that material can be restricted to those authorised to see it. Only DII Standard users will be able to access material held within Meridio.

SharePoint Team Sites , Document Libraries and Site Extenders (including MOSS)

16. The main collaborative working environment on DII is Microsoft SharePoint (often called MOSS in the SharePoint 2007 version). Content of several different types can be hosted in SharePoint, mostly in Team Sites (a set of web pages linking to documents, lists, meeting workspaces, etc.). Team sites are structured according to the needs of individual teams in response to their role.

17. Team Sites and any subsidiary stores of information (including Document Libraries) are controlled locally. They are by default made available to all DII Standard users, although access can be restricted through the setting of permissions; it should be noted that DII Occasional users cannot access any Team Site. Their main purpose is to help team members work together, so the material you store there should normally be for the use of the people who work in your team, or for those other people with whom they work closely. When setting permissions, remember the target audience – neither make material available to a universal audience when access should be restricted, nor block access to people who should be able to see it.

18. A Team Site should contain all the relevant documents generated by that team (or by others directly relating to the work of that team). These may include working documents, internal processes, agendas and minutes of meetings, project plans, progress reports, email messages, etc.

19. Any item on the team site that needs to be preserved as a record of business, should be stored in Meridio (or the unit's approved alternative, usually NTFS) – if a document is correctly declared to Meridio as a record from a DII teamsite, a link will be retained, so that the record can be accessed readily from the teamsite. This ensures people can still see the full story from the team site, while the important material is secure against amendment or deletion.

20. Site Extenders are areas of NTFS storage attached to Team Sites, when for some reason (e.g. certain file types, large files) they can't be included within the Team Site itself.

Windows NTFS Shared Storage

21. NTFS (sometimes called GFS) is the traditional Microsoft file storage environment, providing shared access to information. (NTFS stands for New Technology File System, although as it dates back to the 1990s, it is now rather old technology). It provides the same hierarchical folder and document view as you will find in "My Documents", but with comprehensive access permissions to make it suitable for shared storage. Before the roll out of Meridio, units used NTFS for storing all significant material, and much material from our recent past is still held there.

22. Defence Records Management Policy mandates that there should be two separate file plans for the items stored in NTFS, one for documents and one for records. Documents and records must only be stored at the lowest level of the hierarchy, so avoid placing items in a folder which has subordinate folders.

Defence Gateway services

23. The Defence Gateway is run by Army Information Systems, and unlike DII, it is accessible from any Internet-connected device. It provides a number of storage environments, including SharePoint 2013, Defence Connect (Enterprise Social Network), and MODBOX (for transferring information between DII and personal devices). It also houses some reference material, including the Acquisition System Guidance. It's not an environment for important MOD documents (except where these are copies provided for external access, as is the case with ASG for instance) – such material should be transferred back into the appropriate DII-hosted shared areas.

Microsoft Outlook

24. Microsoft Outlook is powerful, easy to use and, unfortunately, can be highly dangerous from an Information Management perspective. Avoid using it to store rich information content. Include the important content in a standalone document, store it in the appropriate shared area (eg team site), and just send a link to it instead. (If the addressees are outside MOD, or within MOD but without access to the right shared area, then an attachment will be necessary).

25. Do not use Outlook as a local filing cabinet. Make sure all significant items of Defence information are placed in the right shared area, with the appropriate access privileges granted.

26. Do not create .pst files (Outlook Personal Folders file) – the technology might let you do it, and unfortunately the DII quota management message even suggests that you should, but don't. Using .pst files is very bad practice, as the information becomes almost impossible to find for anyone except the person who put it there.

My Documents (local filestore)

27. Role Folder(s) - Only use your Role file folder(s) as a scratchpad for temporary work files, such as quick notes for your own benefit or as a temporary location for sensitive information until such time as it can be transferred into a Team Site with suitable access permissions applied. As soon as any significant effort has been spent on something (rule of thumb – an hour or two's work) and the information within it gains value to others as well as yourself, move it to the right shared area (eg SharePoint team site). **Never** store your personal files here.

28. Personal folder(s) - Only use your Personal file folder to store your own personal (work related) files – for example: course notes, CVs, Job applications, etc. **Never** store work that is of direct relevance to your team or unit here (unless the sensitivity dictates its use until such time as it can be transferred into a Team Site with suitable access permissions applied).

Off Line Storage (CDs / DVDs / Memory Sticks, etc.)

29. Never store the main copy of a document or file in offline storage. CDs/DVDs/Memory Sticks and other off-line storage media are really only useful for transporting information from one ICT environment to another, but even then only when people use them properly, and follow all the instructions about encryption, labelling, and carriage).

Laptops

30. DII laptops provide the facility of local copies of information, so that it can be worked on when disconnected from the main networks. They should not however to be used for long-term storage – information should be regularly synchronised back to the appropriate storage area at the first possible opportunity.

Places not to store information

31. There are several places where you shouldn't (knowingly) store material, including:

- **Local Hard disk (C: drive)** - Your DII system automatically saves items to your C: drive (usually within your profile area). This is a normal system processing routine. **However, you should avoid doing the same yourself**. Don't save files to your hard drive;
- **Desktop -** Don't store information here. Only use it to organise and display your application icons and shortcuts;
- **Recycle Bin** - Don't use your Recycle Bin to store items (but make sure it is regularly emptied);

- **Non-government systems** – Don't store Defence information on home or other privately owned computers. Although the Defence Security Guide allows use of some privately owned computers for processing official information under certain conditions, it is not a suitable environment for storing information – official shared areas should be used. Also note that official information held on private computers (or in personal accounts on commercial email systems, etc) is also covered under the Freedom of Information Act – see Information Commissioner's Guidance here).

32. Remember, as stated earlier, that although Outlook, My Documents, and Off Line Storage have their uses, they are not the places to store information of relevance to your team or unit. The core of MOD Information Policy is the proper use of Shared Areas (mainly Intranet, Meridio, and SharePoint Team Sites (or Windows NTFS for people who don't have SharePoint and Meridio).

Searching for Information

33. One of the main purposes of storing information correctly is of course to enable people to find it readily. The DII Enterprise Search will search the Defence Intranet, Meridio, and Team Sites (obeying any access permissions set). Outlook and My Docs are usually only searchable by the account holder – a key reason why these are bad places to store significant information.

34. Where information is held in other environments, such as the Defence Gateway services, then the local search facilities need to be used. MOD's Internet sites also have local search, and of course Internet search engines can be used.

Summary of Main Storage Areas accessible from DII, and their Primary Purpose

Environment	Breadth of Interest	Access Requirements	Business Significance	Mainly for …
Internet	Global	Fully open (worldwide)	Yes	Unclassified information to be published to the world
Defence Collaboration Programme Sites	MOD & Industry	Limited (inside and outside MOD)	Yes	Secure collaboration with industry
Defence Intranet	Pan Defence	Fully Open (within Defence)	Yes	Info to be published across Defence
Meridio (or other Records store)	Any	Open or limited	Yes	For preservation of MOD records … explaining what has been done, and why
SharePoint Team sites / Site Extenders / NTFS	Local (or wider)	Open or limited	Yes	Normal working environment .. all info of business significance to be here (sometimes in form of links to Meridio or other records store)
Windows NTFS	Local (or wider)	Open or limited	Yes	Interim system for units when they were without SharePoint / Meridio.
Defence Gateway	MOD personnel	Open (within Defence) or limited	Transitory *	Services designed for access by Defence people using non-MOD devices (as well as from MOD)
Outlook	Local / Personal	Individual (& any delegates)	Transitory *	Short communications, alerts to info held in shared areas, external communications (but if it's significant information, move emails & attachments to shared areas
My Docs (Role)	Personal	Individual	No	Scratchpad for notes or other temporary work files, of no real value to anyone but yourself.
My Docs (Personal)	Personal	Individual	No	Personal material (eg career related, courses)
Offline storage	Local / Personal	Whoever has the storage device	Transitory *	Transit only … not permanent storage
Laptop	Local / Personal	Whoever has the device	Transitory *	Remote access / disconnected working … not permanent storage

* Significant information to be transferred to appropriate shared area at first practical opportunity

UNDERSTANDING LEGISLATION

Why legislation matters and where to go for help

1. You're expected to comply with the law at all times - ignorance of it isn't a defence. If you break the law at work, you're likely to face legal and MOD disciplinary action, and the department may also be brought to book. The MOD doesn't expect us all to be legal experts, but it does expect us to take care when working with information (and using information tools) and to seek expert advice when we're not sure if what we're doing is legal. If you're in any doubt. For advice on legal issues and how they could affect you at work, contact the MOD's Central Legal Services (CLS) team.

The basic ground-rules

2. Always:

- **potect information properly**. Under the **Data Protection Act 1998**, you're expected to protect personal information, irrespective of where or how it's held. Extra care is needed when handling sensitive personal data. For example, sensitive personal information - as defined by the Act - can only be used with the explicit permission of the data subject. For further details refer to the MOD's Data Protection Act guidance. The **Official Secrets Act** is also important – you should have completed an Official Secrets Acts & Confidentiality Declaration on joining the MOD – so don't breach it by disclosing information you're not allowed to;

- **behave properly when working with Information (and supporting tools)**. Make sure you abide by the MOD's Acceptable Use Policy (JSP 740). It sets out the standards of behaviour expected of you when you use the MOD's information tools or work with information. Many of the activities outlawed there are unacceptable whether you're using IT or not;

- **bear in mind that members of the public may be allowed access to the MOD's information**, including material you've produced (electronic or otherwise) at work. The **Freedom of Information (FOI) Act 2000** gives people a general and retrospective right of access to the MOD's information, irrespective of the format the items are held in. We are obliged to respond to all FOI requests, and release the information unless a specific exemption replies. It is a criminal offence to deliberately destroy, hide or alter requested information to prevent it being released.

- For further information refer to the MOD's FOI guidance. The **Public Records Act 1958** and the **Civil Evidence Act 1995** also come into play.

More about the legislation

3. Many pieces of legislation – some with sections which apply to individual nations within the United Kingdom – apply to us when we work with information (and when we use the supporting tools). We've summarised the main pieces of legislation below. Find out more by referring to the transcripts of the UK Acts of Parliament or – as they're not that easy to understand – refer to the Justis website instead. We've also produced a summary of the four main Acts you need to know about.

- The **Civil Evidence Act 1995** makes public documents and records of a business or public authority admissible as evidence in civil proceedings, and thus available for disclosure. So, it's possible that something you've produced (electronic or otherwise) could be disclosed in the future.

- Under the **Communications Act 2003**, people making improper use of a public electronic communications network may be guilty of an offence. This includes sending or causing to be sent, a grossly offensive, indecent, obscene, or menacing message: or for the purpose of causing annoyance, inconvenience or needless anxiety, sending or causing to be sent, a false message or persistent use of a public electronic communications network.

- The **Computer Misuse Act 1990** makes it an offence to gain or attempt to gain, unauthorized access to, or carry out any unauthorised modification of, a computer system or data stored on it.

- The **Copyright, Design and Patents Act 1988** applies to all information and makes it an offence to breach copyright. It's easy to do this without realising, because accessing, copying and distributing information held electronically is usually straightforward.

- The **Data Protection Act 1998** is designed to safeguard personal data (i.e. about a person), and it expects each of us to handle it properly and responsibly, irrespective of how or where it's held. It is based on eight core principles, all about ensuring that data held is accurate, carefully protected, not excessive, and not used inappropriately. If data - as defined by the Act – is sensitive, it can only be used with the explicit permission of the data subject.

- Under the **Defamation Act 1996**, in an action of defamation, the person who is the author or publisher, or who causes the publication of a defamatory statement, may be personally liable. Publication can be as simple as sharing a defamatory statement made by one person about another with a third person (in a letter, in an email, by voicemail, on a statement posted on the internet, etc).

- The **Environmental Information Regulations 2004** provide public access to environmental information held by public authorities (closely allied to FOI).

- The **Equality Act 2010** requires equal treatment in access to employment and services, regardless of age, sex, religion, disability, etc. Also, the MOD is required to make reasonable adjustments to help disabled people overcome barriers in the workplace

- The **Electronic Communications Act 2000** provides for the admissibility in legal proceedings of electronic signatures on electronic communications such as emails.

- Participating in a chain-gift scheme might be an offence under the **Gambling Act 2005**.

- The **Human Rights Act 1998** upholds the qualified right to respect for private and family life. So, each of us must respect this when we handle, store and share personal information.

- Under the **Malicious Communications Act 1988** it is an offence to send communications containing indecent, grossly offensive, threatening or false information, so as to cause distress or anxiety.

- Disclosing information in breach of the **Official Secrets Acts 1989** is an offence.

- The Protection from **Harassment Act 1997** makes it an offence for a person to pursue a course of conduct (abusive communications, say) that amounts to harassment of another (and which that person knows or ought to know, amounts to harassment).

- The **Protection of Children Act 1978** makes it an offence to possess indecent photographs or pseudo photographs of children with a view to them being shown or distributed.

- Under the **Welsh Language Act 1993** and the **Welsh Language (Wales) Measure 2011**, MOD (along with other public authorities) is required to treat the Welsh language and English language on the basis that they are equal when conducting business with the public in Wales, and to enable members of the public to deal with the department through the medium of the Welsh language if they choose to do so.

UNDERSTANDING COPYRIGHT

About Copyright

1. Copyright is the exclusive right to produce copies of a piece of work – including books, films, TV and radio programmes, music and other sound recordings, newspapers, magazines, software programs, databases and web sites. Under the Copyright, Designs and Patent Act 1988, if you're not the copyright holder, you're not allowed to produce copies of a work unless you have a special licence to do so. **Infringing copyright is against the law** and it's also a disciplinary offence here to knowingly copy, store, distribute or transmit material obtained in breach of copyright. If the MOD (or the Crown) doesn't hold the copyright, and it hasn't obtained specific approval to copy or store material, it's breaking the law.

2. Although the Act grants several general authorisations to use copyright works (e.g. for educational purposes), they're limited in scope, so make sure of your ground before you decide to use them. It's possible that the MOD or Crown already has a licence agreement (secured under a procurement contract, for example) in place with the copyright owners - covering copying (local or general), storing, limitations of use, etc - for various items, including:

- publications related to equipment it's purchased;
- reference documents supplied by its libraries;
- specified documents;

3. The works we produce here are covered by Crown Copyright, so we are allowed to use them, make copies of them and store them on MOD systems. The same applies (in most cases) to works produced by other departments, but if in doubt, check with the originating department first.

4. In general, where copyright material belongs to a third party, **you must not copy or store it on MOD systems without permission from the copyright owner**. Permission is usually in the form of a written/printed licence from the copyright owner, which helps the MOD to prove its rights. Here are a few instances where, if the MOD hasn't been specifically given permission to copy, store or use copyright material, you'll almost certainly be infringing copyright:

- Buying music on a CD or by download, taking a copy and placing it anywhere on our systems (including in personal storage);
- Taking an extract from a DVD of a film or TV programme without permission and then reusing it (building it into a presentation, say);
- Copying cuttings from newspapers and magazines.

What you need to do

5. **Always abide by the Act**. If you:

- are retaining items on a Defence system in breach of copyright, remove them now. If colleagues are in the same situation, ask them to do the same (or ask a person with responsibility for information in your unit (e.g. Information Manager) to tell them;
- are responsible for tidying up information storage and removing unauthorised copyright material in your unit, target music, images and video. Check large files with extensions such as AVI, MOV, MP3, MP4, MPEG, MPG, WAV, WMA and WMV, as well as other large files, just in case the file extension has been changed to conceal the type of file, but be careful. Just because a file has one of those extensions doesn't necessarily mean that it's an unauthorised copy;
- are thinking about using and storing new third party copyright material on MOD systems:
  - make sure a legitimate business need exists;
  - check whether the requirement can be satisfied using a MOD originated Crown Copyright work instead – for example: try referring to the MOD Defence Image Database for photographs you can use - and if there isn't another option, make sure you have a licence (whether new or existing) permitting you to do what you want to do

before you start. Do this by checking the source of the work; for example, if the work was supplied by a contractor, check the terms of the procurement contract. If there isn't a contract and you can find no evidence of a licence being granted to the MOD, you must assume that the MOD (you) doesn't have the right to use the material. If you decide to contact the copyright owner to find out if they're prepared to grant permission, be aware that the MOD could incur a charge.

- want to use cuttings, check with your on-site library (if you have one), or the Defence Business Services Library and Digital Services team, to see if the MOD already subscribes to a service you can use. The MOD also has a limited licence to enable some ad hoc photocopying and scanning of newspapers and magazines for official purposes, and details of this licence can be found in 2005DIN01-010 (Guidance on copyright licences for photocopying and scanning). However, if the newspaper is published on the web, and you and your colleagues have internet access, then you can safely send a link to the article – just don't copy it out wholesale;

- wish to use third party music or videos, the easiest way to obtain a licence is usually to contact one of the Collecting Societies set up to collect licence fees on behalf of copyright owners. You can find a list of the most relevant collecting societies in Copyright and Crown Copyright material: Policy, Responsibilities and Procedure for use (2011DIN05-044), with a more comprehensive list on the Intellectual Property Office's pages on gov.uk - list here;

- decide to take a licence for third party copyright (other than under a procurement contract using the IPR DEFCONs), **obtain authority from the Defence Intellectual Property Rights team (DIPR**) (at DGDCDIPR-DR@mod.uk) **before you sign the licence**. Make sure that you also pass a copy of the license to DIPR for its records, to help the team there respond to license related enquiries (from licensing bodies, copyright holders, etc) received by the MOD;

- wish to report a suspected copyright infringement, contact DIPR;

- need expert advice on copyright or licensing issues, contact DIPR

SHARING SERVICE POLICE INFORMATION IN SUPPORT OF PUBLIC PROTECTION AND THE PREVENTION AND DETECTION OF CRIMES

Audience – All personnel responsible for the handling of Service Police Information.

Introduction

1. As the Service Police (SP) do not have a statutory duty to co-operate under the Criminal Justice Act 2003, Multi-Agency Public Protection Arrangements (MAPPA), the effective sharing of information by the Service Police with partners in the law enforcement community, as well as others, is key to the effective prevention and detection of crime and protection of the public. This policy only refers to the sharing of SP information (See paragraph 3 below).

Definitions

2. **Information Sharing.** Information sharing is the processing of information either on a one-off or an ongoing basis between partners for the purpose of achieving a common aim.

3. **SP Information.** SP information is any information that is gathered and held by the SP for a policing purpose. It does not include crime statistics or general SP administrative information.

4. **Policing Purpose.** A policing purpose is:

   a. protecting life and property;

   b. preserving order;

   c. preventing the commission of offences;

   d. bringing offenders to justice; and

   e. any duty or responsibility of the SP arising from common or statue law.

5. **Personal Data.** Personal data is that which relates to a living individual who can be identified:

   a. from those data; or

   b. from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect to the individual.

6. **Sensitive Personal Data.** Sensitive personal data is personal data that relates to an individual's:

   a. racial or ethnic origin,

   b. political opinions,

   c. religious or other similar beliefs,

   d. membership of a trade union,

   e. physical or mental health condition,

f. sexual life,

g. alleged or committed criminal offences, or

h. proceedings for any offence committed or alleged to have been committed.

Statutory Obligation to Share Information

7. The SP have a statutory obligation to disclose information to the Child Support Agency (CSA) and Disclosure and Barring Service, as well as that subject to a court order. In addition, there is also a statutory obligation, subject to the appropriate exemptions, requested under the Data Protection Act 1998 (DPA) and Freedom of Information Act 2000 (FOI).

SP Police to Police/Law Enforcement Agency Disclosure

8. **DPA Exemptions.** SP information can be shared with UK Home Office Police Forces and other law enforcement agencies provided the Sect 29 (Crime and taxation) or the Sect 35 (Disclosure required by law or made in connection with legal proceedings) DPA exemptions apply.

9. **Requests for SP Information.** All requests for SP information must be processed by the Service Police Crime Bureau (SPCB), utilising the appropriate 'Request for Information (RFI)' application form (Annexes A to C). The RFI must specify why the information is required and it must be counter-signed by the supervisor[1] of the requester. SPCB will maintain a record of all RFIs received and subsequent SP information disclosed.

Disclosures to non-Police/Law Enforcement Agency

10. **Requests.** Where there is no statutory duty to disclose SP information to non-Police/Law Enforcement Agencies, each request must be carefully considered to ensure that any disclosure is compliant with DPA. All requests must be made to the SPCB, who will ensure that it has been made with the appropriate authority and that the reasons for the request meet the requirement for an exemption under Sects 29 or 35 of DPA and the additional conditions in the case of sensitive personal data. In most cases, requests for SP information are likely to be necessary for the administration of justice and so will meet these requirements. However, should there be any uncertainty that a requirement for DPA exemption has been met, the request should be forwarded to the single Service Deputy Provost Marshal (DPM) for advice.

11. **Service Police Disclosures.** There may be occasions when it is considered necessary, usually for public protection purposes, that the SP disclose SP information proactively with a non-policing or law enforcement agency. On such occasions, any disclosure must be authorised by a single Service DPM, who will be acting on behalf of the appropriate Provost Marshal (PM)[2]. In deciding whether to authorise the disclosure, the DPM will consider the following:

a. Has the person to whom the information relates (most commonly the person suspected of committing an offence) consented to the disclosure of the information? If so, should the suspect be approached and requested to consent? Information may be disclosed without consent provided that it meets one or more conditions under Schedule 2 of the DPA, and in the case of sensitive personal data, Schedule 3.

b. Can it be argued that due to any threat to public protection, the SP may be obliged by articles 2 (Right to life) or 3 (Freedom from torture or degrading treatment) of the Human Rights Act 1998 to disclose the information? This must be balanced against the rights of any person suspected of an offence – notably articles 6 (Right to a fair trial) and article 8 (Right to

[1] For UK civil police the minimum Supervisor rank is Inspector.

[2] For DPA purposes each single Service PM is acting on behalf of the Data Controller, the Secretary of State for Defence.

privacy). The key consideration is whether the purpose for the disclosure justifies the infringement of the suspect's rights?

c. Is there an over-riding public interest or duty to the public in the disclosure of the information?

12. In all cases, only the SP information that is proportionate and necessary to meet the requirement should be disclosed. In addition, extreme care must be taken to ensure that the identities of others that are unconnected to the matter are not disclosed and that any anonymity of victims, statutory or otherwise, is strictly observed.

Enduring or 'Wholesale' SP Information Transfers

13. Should there be a requirement to initiate an enduring requirement to share SP information with a partner or undertake a 'wholesale transfer' of data; the arrangement should be subject to a Data Sharing Agreement (DSA). All DSAs should be drafted and authorised by the appropriate single SP HQ Information Manager on behalf of the Data Controller. The use of a DSA will:

a. Create a formal arrangement for the information sharing within terms of reference.

b. Ensure that appropriate conditions are placed on the manner in which the information is handled, stored and used by both parties.

c. Ensure consistency and compliance.

d. Build confidence in displaying robust information management in the protection of the public.

Subject Access Requests

14. Sect 7 of the DPA gives the right for individuals to access personal information held by organisations about them and to request copies of that data. These are known as Subject Access Requests (SARs). All SARs are to be forwarded to the SPCB, who will consider whether any DPA exemptions apply and respond with any necessary disclosure on behalf of the Data Controller. All SARs must be responded to within 40 calendar days.

Point of Contact

15. Any questions or queries regarding this policy should be directed to:

SO2 Service Police Policy, 6.K.49, Discipline, Conduct and Legislation Team,
Defence People Secretariat, MOD Main Building, Whitehall, London, SW1A 2HB.

Email: People-Sec-DCLSvcPolicePol@mod.uk
Tel: (Mil) 9621 84815 (Civ) 020 7218 4815

CONDUCTING PRIVACY IMPACT ASSESSMENTS

Privacy by Design

1. The Data Protection Act applies every time that we process information that relates to living and identifiable individuals (personal data). If we do not protect that information adequately, we risk breaching the Act. The department could suffer reputational damage or face legal action which in some circumstances, could lead to fines. Additionally, in extreme cases, the Department or staff involved may be committing a criminal offence. Privacy by Design is an approach to projects that promotes privacy and data protection compliance from the start.

2. We should adopt Privacy by Design for projects which are likely to be handling personal data, for example:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

Privacy Impact Assessments

3. A Privacy Impact Assessment (PIA) is a process that we can use to identify and reduce the privacy risk of our projects. A PIA can also reduce the risk of harm to individuals through the misuse of their personal information. It can also help us to design more efficient and effective processes for handling personal data. The PIA approach is sponsored by the Information Commissioner's Office (ICO) for use by any organisation – not just Government.

4. Detailed guidance is published by ICO in Conducting privacy impact assessments code of practice. This document advises why and when PIAs should be undertaken, and how to do them. It also provides a template which can be used to record the PIA process and results (at Annex 2 in version 1.0). It is not necessary to use this exact format, but it does make sense to answer all those questions posed – they are intended to save time and trouble further downstream. For MOD guidance, refer to Undertaking PIAs in the MOD and 2010DIN05-065 Requirements for PIAs. These can be used in conjunction with the aforementioned ICO guidance.

Obtaining further advice

5. The Data Protection Officer for your unit or TLB should be the first port of call. Accreditors of ICT systems will also be very interested.

UNDERSTANDING THE ROLE OF THE INFORMATION ASSET OWNER

Introduction

1. The role of Information Asset Owner was introduced across Government, following a report on Data Handling Procedures in Government (2008). The aim is to make sure that we manage our most important information assets carefully, reducing the risk of loss or inappropriate disclosure of data, while making good use of the information that we have. The role is mandatory in Defence.

What is an Information Asset, and what is the Role of the information Asset Owner (IAO)?

2. These are the Government definitions:

> *"An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles."*
>
> *"Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process."*

Guidance to IAOs, and associated Training

3. The Cabinet Office publishes Guidance on the IAO Role, available on GOV.UK. This is the authoritative document for use in Defence. All IAOs should be familiar with it, and follow its advice unless they have separate instructions from their TLB HQ.

4. The National Archives (TNA) is responsible for delivering a training and engagement programme for Information Asset Owners. TNA have suspended face to face training with effect from Spring 2016 while training material is refreshed, and an announcement on the resumption of training will be available on their website later in 2016. In the meantime, self-study of the Cabinet Office Guidance should be undertaken by IAOs.

Obtaining further advice

5. The Data Protection Officer or Senior Information Risk Officer within your TLB should be the first port of call.

MANAGING INFORMATION IN DATABASES

Databases - what are they and what are they for?

1. When people talk about databases, they're usually referring to a collection of electronic data organised in such a way as to be managed, accessed, updated and interrogated using Database Management System tools. They offer powerful search capabilities, often allowing us to obtain results quickly to complex queries. They're not necessarily easy to design, build, maintain, document and support, so the people involved need specialist skills. A robust, well-designed database can be very useful, but it should only be used where it's cost effective to do so, with the benefits of use justifying the investment in management resources and technical skills - and where your business requirement cannot be satisfied by a simpler solution.

2. Good design is vital. Without it, performance and reliability (availability, accuracy, etc.) will be impaired. So, we don't advocate the use of local do-it-yourself databases. They're not an easy option. All of the standard MOD information policy commitments, rules and standards apply, and you also need to consider data interoperability requirements. To continue to meet business requirements, a database relies on the people who manage and use it having a good understanding of how it works, together with the skills to maintain and improve it. People need the time, the right access permissions and skills (including knowledge of good practice) and the authority to do the job properly.

What major applications does the MOD use?

3. The MOD has enterprise agreements with various database application vendors, but there will be database systems out there not supported by a formal agreement. So, check to make sure the application you're planning to use is covered by a valid agreement. In all but the most exceptional cases, it isn't a good idea to use one that isn't covered, unless you're confident that the advantages outweigh the risk of a system failure or problem.

What are the skills required?

4. A team involved in developing, managing and maintaining a database should have:

- a clear understanding of the requirement;
- business analysis and design skills;
- data analysis and design skills;
- programming experience in the relevant application; and
- an appreciation of the potential lifecycle of the system especially if it is likely to be business critical or experience considerable growth.

Getting Started

5. Before starting work, you need to get formal approval to do so, in line with local procedures. You may need to produce a Project Initiation Document to:

- identify the responsible owner who endorses the business requirement and is going to be responsible for monitoring use (successes, benefits, costs, etc.);
- set out all through-life resource requirements - to maintain continuity of support, documentation, etc.;
- set out the types of information to be held, the people who will be given access, and the management of those access permissions;
- explain how the information will be protected from inappropriate access or disclosure; and
- summarise anticipated developments.

6. Only implement a database if you're sure that there are specialist resources available to maintain and develop it throughout its life.

What should you consider when choosing a database?

7. Understand, and be clear about, the requirement. Know the information you need. Make sure you know where to get it, how to get it and how you're going to use it.

8. When selecting a database product, there are several things you need to factor in, including:

- the number of concurrent users – i.e. the number of users using the database at the same time;
- the number and size of tables;
- the complexity of the functionality;
- the network connectivity – the location and geographical spread of the users may put particular stress on networks, which can be reduced by the more sophisticated data handling of higher end applications;
- security requirements – less capable applications characteristically lack secure data handling and recovery functionality;
- data sources – the complexity of data capture and interfaces with other systems;
- the different levels of access required – will all users be able to see all of the data on the database, or should some users (e.g. contractors) be given limited access permissions?
- scalability issues - what's the likelihood of the system ending up with having wider applicability in the long term (with an expanded user base) or becoming business critical? Have the original copyright/confidentiality requirements changed? If they have, you will need to make sure that you have secured the right to share the database information with the new users (especially if the database contains third party information and users include non-MOD employees (e.g. contractors).
- the network topology – the use of remote servers can lead to impaired system performance, so locating them closer to the users (using Local/Metropolitan Area Networks, say) may well work better.

Scaling Up

9. You may well need to convert from one database application to another if the database grows significantly, the user population grows, or the underlying network changes. More often than not, it's easier to stay with the same family of database applications. With so many variables involved, it's impossible to give a one-size-fits-all answer on when you need to migrate, but here's a good rule of thumb - if there are now more than ten users or more than 100MB of data, it's probably time to convert (or at least start thinking about doing so). However, so much will depend on things such as the network topology and the usage volumes.

Protecting Data

10. Data security is important. Protect information in line with its protective marking. Large amounts of even unclassified data may, when aggregated, provide a picture of our activity which could lead to serious consequences if it falls into the wrong hands. Only load data onto a database when you are certain that the MOD has secured sufficient user rights to do so. Before granting people access to a database, the database administrator should make sure that they are entitled to see all of the data held. If they are not, they must deny them access.

11. Don't store unnecessary personal data just because you can. Look after and protect ALL personal data (not just items such as National Insurance numbers, bank account details, and passport and driving licence numbers) to avoid causing distress and to protect people against the risks of inappropriate access and loss, identity theft and fraud, using formal security caveats to give additional protection to information which may compromise someone's security or safety.

12. If you are intending to store or access personal data, you will almost certainly need to undertake a Privacy Impact Assessment – our guide on Conducting Privacy Impact Assessments (Info 28) sets the scene. This will be a slight overhead at the start of your project, but could well save you a great deal of time and trouble later. Always comply with the Data Protection Act and MOD instructions on holding personal data (refer to our guide on Handling Information Requests (Info 12), for example).

13. Remember that the Freedom of Information Act and Public Records Act apply, and Intellectual Property Rights and commercial confidentiality restrictions may also apply.

Back ups

14. The data is important. It's trickier to recover a corrupt database than a corrupt flat file, so make sure that regular backups are taken. Where it supports automatic back-ups, configure the application to take them at regular (appropriate) intervals. Small applications may well need to be backed up manually - one approach is to close the system for back up at the end of the working day or before start of business in the morning. Backup security is every bit as important as database security.

Conclusion

15. Database projects are often easier to start than to maintain or to finish. Modern technology provides excellent tools, but think carefully how the project (and the information) can be effectively managed through life before making that commitment to start it.

ELECTRONIC RECORDS MANAGEMENT PROCEDURES

Introduction

1. This guide contains guidance for business units using a formal Electronic Records Management System (ERMS).

FILE PLAN FOR AN ELECTRONIC RECORDS MANAGEMENT SYSTEM

Background

2. The ERMS file plan should define a hierarchical filing structure into which individual records are filed. 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.

What you should do

3. File plans must be created and maintained by the business unit iHub staff following this guidance. 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.

- A class can contain other classes or folders, but never records.
- 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.

OPENING AN ELECTRONIC FOLDER

Background

4. 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.

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

6. 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.

What you should do

7. A folder must not be opened until there is an enclosure to be placed in it. The folder title and designated file number (if used) must be described clearly. An owner must be assigned to every new folder. This is to assist with the eventual disposal of the folder.

8. The class and folder hierarchy must have a retention schedule associated with it. The approved retention schedules for electronic folders are:

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

9. At least one definition from the Defence taxonomy must be applied to the folder. At least one definition from the Defence File Plan must be applied to the folder.

10. The folder must be set to automatically create new parts. The folder part must be set to close after 100 enclosures.

11. 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 security classification) to be linked.

DECLARING RECORDS INTO ELECTRONIC FOLDERS

Background

12. 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.

What you should do

13. 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 JSP 441 Guide Records 02, Paper Records Management Procedures, 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.

14. There are other items that can not be stored in the ERMS. These records may be in a range of formats including maps, plans, drawings, charts, video, film, photographs, etc. See other JSP 441 Guides for details.

Contents of an Electronic Folder

15. 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 Annex A of JSP 441 Guide Records 04, Records Review Process for Desk Officers.

16. All records declared in to the ERMS must comply with JSP 441 Guide Info 07, Naming Documents and Records.

17. 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

18. 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.

MANAGING TOP SECRET ELECTRONIC RECORDS

19. Unless using a system approved by the Departmental Record Officer, 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 JSP 441 Guide Records 02, Paper Records Management Procedures.

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

21. Business units must not destroy folders containing TOP SECRET records. Access to these must be passed to the DBS KI Records Review team once they have reached their retention schedule and cease to be of business use.

WEEDING OF ERMS FOLDERS

22. 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; The National Archives requires MOD to select complete folders for permanent preservation rather than extracts from folders.

CLOSING AN ELECTRONIC FOLDER

Background

23. 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:

- The folder part contains 100 enclosures;
- 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);
- Action on the subject covered by the folder has come to an end.

What you should do

24. 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.

PAPER RECORDS MANAGEMENT PROCEDURES

Background

1. This guide contains procedures specifically relating to the management of paper records. Generic records management procedures are contained in other 'How To Guides' available on the Information Portal.
2. Business units may still generate paper records and use paper filing systems. Some business units use hybrid records management systems, where some records are managed in a paper form and others managed as digital records in an Electronic Records Management System (ERMS). Business units may also receive material in hard copy and on occasion it will not be possible or practical to digitise the material through scanning. For example, if the original needs to be kept for contractual purposes, or if there is a large volume of material.
3. You must ensure that material which is deemed worthy of retention is filed on a registered file as soon as possible and its existence recorded in an ERMS, if available.

OPENING A REGISTERED FILE

4. A registered file should be opened as soon as there is an enclosure to be filed on it.
5. Purpose-designed registered file covers (listed below) must be used and are to be ordered from Logistic Services Forms and Publications team, using MOD Form 999. Details of the ordering process can be found in DIN 2008DIN04-049 or in Ordering Forms from Forms and Publications.

    - **TOP SECRET** (Red) - MOD Form 329A
    - **SECRET** (Pink) - MOD Form 329B
    - **OFFICIAL** (Buff) - MOD Form 329D

6. When opening 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 part numbers 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 existence of the registered file should also be recorded on the ERMS, where the unit has implemented one.

The Registered File Record Sheet (MOD Form 262A)

7. When a new registered file is opened its existence must be recorded on a Registered File Record Sheet (MOD Form 262A).
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).

The File Minute Sheet

9. The file minute sheet is a plain piece of A4 paper that is held on the left hand side of the registered file. Each minute sheet should be numbered and the security classification 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.

10. 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.

Security Classification

11. The security classification of the registered file cover is to correspond to the highest security classification marking of its contents. For example, a file classified as TOP SECRET may contain a majority of information classified OFFICIAL and only one TOP SECRET document. Should an OFFICIAL file exist and a new document classified as SECRET or above need to be placed on it, the file is to be upgraded.

PLACING DOCUMENTS ON A REGISTERED FILE

12. 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 on the top right hand side of each enclosure sequentially numbered, for example E1, E2, etc. An enclosure stamp or a red pen can be used.

13. Late enclosures should also be filed in date of origin order. This will mean inserting them between existing enclosures. Existing enclosure numbers must not be destroyed or 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.

14. 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.

Material NOT placed on Registered Files (Unregistered Records)

15. 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.

16. 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.

TRANSFER OF ENCLOSURES BETWEEN REGISTERED FILES

17. Occasionally enclosures will be misfiled to the incorrect registered file and this will need to be corrected. When an enclosure has been misfiled and the action taken 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 document’s reference
- The security classification
- 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

18. 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 security classification marking

- The date of transfer
- The signature of the officer authorising/making the transfer
- The reason for the transfer

TEMPORARY ENCLOSURE JACKETS

19. 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 of appropriate security classification (listed below).

    - TOP SECRET - MOD Form 174A
    - SECRET - MOD Form 174B
    - OFFICIAL - MOD Form 174D
    - They should then be forwarded to the appropriate business unit in accordance with JSP 440, 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 security classification 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

20. 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 recorded in the TEJ. 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

21. Purpose-designed TEJs should be used and can be ordered from Logistics Services Forms & Publications team. See Ordering Forms from Forms and Publications for more details.

TEMPORARILY SENDING REGISTERED FILES TO OTHER BUSINESS UNIT

22. 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 and the date it was received back into the business unit

23. 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.

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

ADDITIONAL PROCEDURES FOR MANAGING CLASSIFIED REGISTERED FILES (SECRET AND TOP SECRET)

25. The main requirements of managing registered files have been described earlier in this guide. However, there are extra procedures that must be followed for registered files classified as “SECRET” and “TOP SECRET”.

26. 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. When an enclosure classified 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).

27. Instructions for maintaining, sending and receiving classified material are contained within JSP 440: The Defence Manual of Security. This guidance also includes details on the completion and management of MOD Form 102.

    Note: The retention period for MOD Form 102 is seven years after its closure.

UPGRADING REGISTERED FILES TO A HIGHER SECURITY CLASSIFICATION

28. It will sometimes be necessary to upgrade a registered file to reflect the fact that a new enclosure is of a higher security classification than the existing file.

29. A new registered file cover of the appropriate security classification must be used and given an identical number to the cover that is to be replaced. (Details for ordering for file covers can be found in DIN 2008DIN04-049 and in Ordering Forms from Forms and Publications).

30. The contents of the original file must be removed and transferred to the new file cover along with the top half of the front of the original cover which should be placed in the new file on the left hand side.

31. The date of opening of the original file must be entered on the front cover of the upgraded file, not the date on which the file was upgraded which instead 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 security classification.

32. 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.

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

34. The enclosure 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: The Defence Manual of Security.

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

DOWNGRADING REGISTERED FILES

36. The regular assessment of holdings of classified registered files should consider whether a current registered file security classification grading needs to be maintained or downgraded.

37. Where it is necessary to downgrade a file to reflect a lower security classification, a new registered file cover of the appropriate security classification must be used and given an identical number to the cover that is to be replaced. (Details for ordering file covers can be found in DIN 2008DIN04-049 and in Ordering Forms from Forms and Publications).

38. The contents of the original file must be removed and transferred to the new file cover along with the front of the original cover which should be placed on the left hand side of the new file.

39. The date of opening of the original file must be entered on the new front cover of the downgraded file, not the date on which the file was downgraded, which instead must be entered in the downgrading section of the original file cover.

40. The corresponding MOD Form 262A must be appended to show the new security classification of the registered file and the date of the downgrade.

41. MOD Form 672 must be amended to show the date of the downgrade and retained in the file.

42. If there is a subsequent need to upgrade the file again then the actions in Upgrading registered files to a higher security classification must be adopted. Where a file has been upgraded previously, the top half of each pre-existing file cover should be retained in the new file.

43. The new classification of the enclosure that triggered the downgrade 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: The Defence Manual of Security.

44. MOD Form 171 – Request for downgrading of classified documents is to be used to record authority to downgrade. This authorisation must be attached to the left hand side of the downgraded file.

DOWNGRADING CLASSIFIED DOCUMENTS

45. Where it is necessary to downgrade an individual document within a registered file to reflect a lower security classification, this action should be done in such a way that the original markings remain legible.

46. MOD Form 171 – Request for Downgrading of Classified Documents is to be used to record authority to downgrade. This authorisation must be attached to the left hand side of the registered file.

47. Once authority to downgrade the document has been received, a marker pen or stamp may be used on the document to reflect the lower classification. The original marking, which must remain legible, is to be crossed through with a single horizontal red line. The document is to be annotated to indicate the date of downgrading (for example, 'This document was downgraded on 13 November 2015').

48. The entry in the Protected Document Register (MOD Form 102) relating to the downgraded document must be amended to show the downgrade action; the MOD Form 102 entry may then be considered closed if the final classification is OFFICIAL.

49. Where a document has been downgraded to OFFICIAL, the container muster list (for permanent accountable documents only [see JSP 440, Part 5, Section 4, Chapter 2, Paragraphs 9-10]) will need to be amended.

50. Where the downgrade affects the classification of the file, follow the steps in [Downgrading Registered files].

MISSING REGISTERED FILES

51. If, after a thorough search, a registered file cannot be located, a written report **MUST** be submitted to the DRO. The report is to: identify the file concerned, its security classification marking and the nature of its contents; and contain an explanation of the circumstances surrounding its loss. If the file contained classified information a report is also to be submitted to the appropriate security directorate in accordance with the instructions in JSP 440: The Defence Manual of Security.

WEEDING OF REGISTERED FILES

52. 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.

CLOSING A REGISTERED FILE

53. 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:

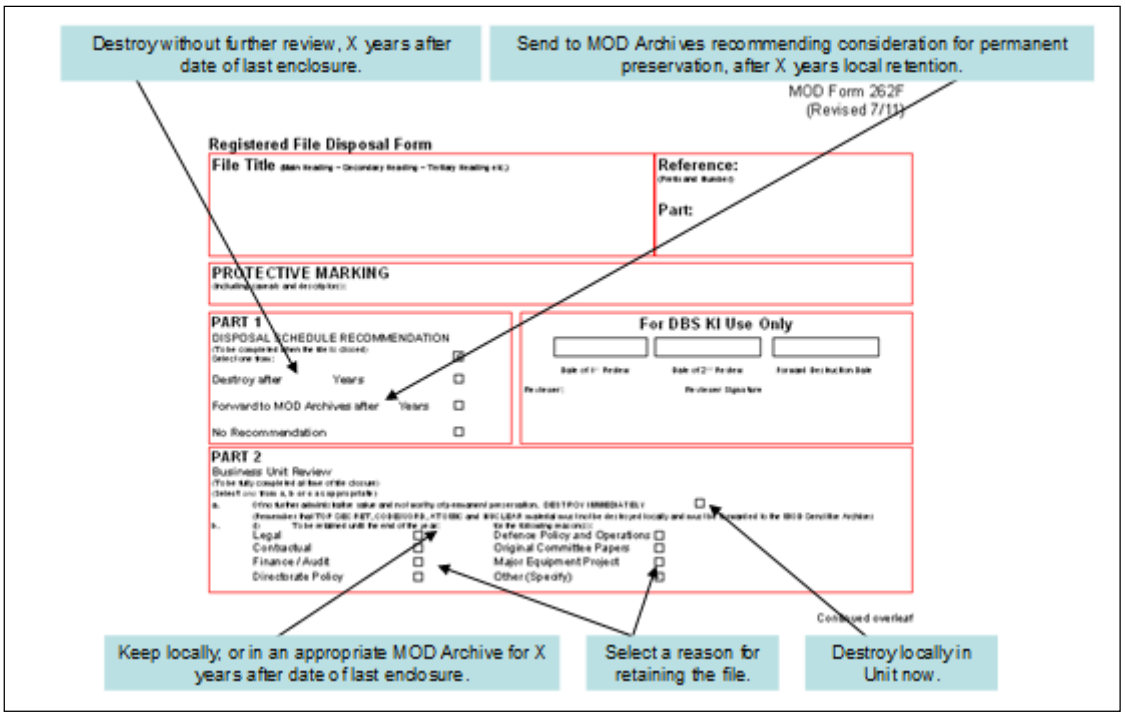
- The file is 1 inch thick
- The file contains 100 enclosures
- The file has been open for 5 years
- Nothing has been added to the file for the last year (close the file unless there is a clear indication that papers will be added to it shortly)
- Action on the subject covered by the file has come to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

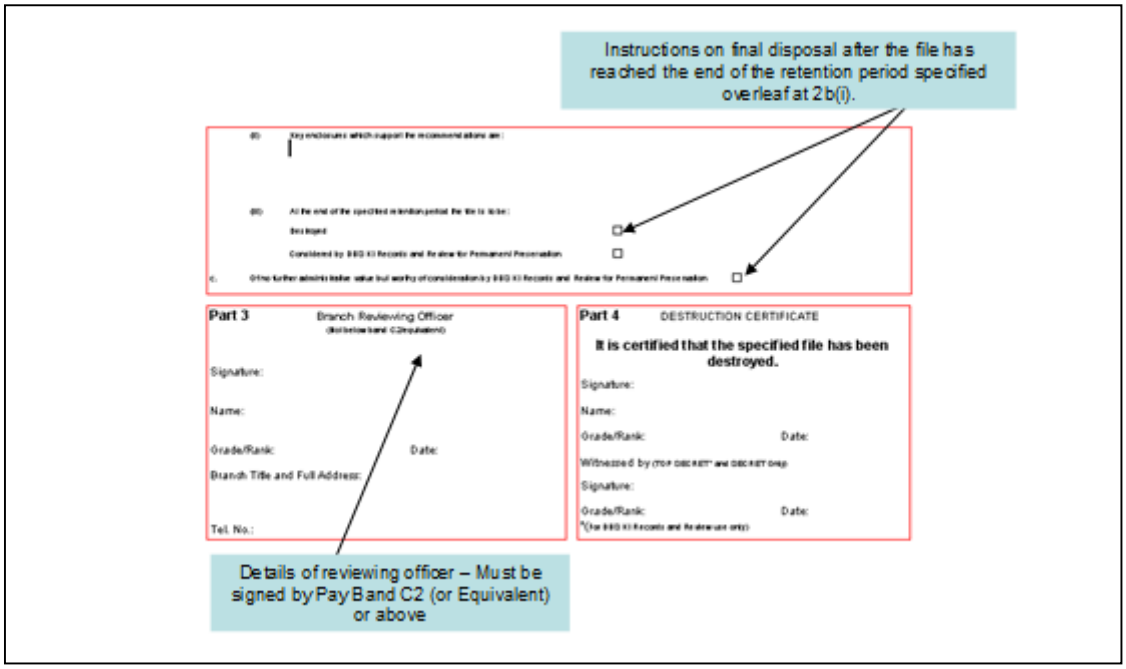
54. The following actions are to be taken when closing a registered file:

- 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
- Create a MOD Form 262F. The file title, file reference, part number, and security classification (where applicable) should be entered on the form along with the date of the last enclosure and the date of closure of the file. Part 1 of the form must then be completed. This records the retention schedule recommendation
- When the file is returned by the "reviewing officer", 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 the archives, 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

55. Further information on reviewing records is included in Records Review Process 'How to Guides', available on the Information Portal.

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





MAINTAINING THE MOD FORM 262A AND MOD FORM 262F

57. 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.

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

59. Each MOD Form 262F must be retained for a period of not less than 20 years from the date of last enclosure (as recorded on the form).

60. 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 20 years following the insertion of the final MOD Form 262F.

61. 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.

62. 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.

63. 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

FILE PLAN FOR A PAPER BASED FILING SYSTEM

64. This guidance should be followed in the rare situation that a business unit has paper records and does not have an ERMS.

65. The file plan should follow a hierarchical structure and incorporate 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

66. 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 dependent on the Organisation or Establishment's key business.

The File Plan - Secondary (or Subsidiary) Headings

67. 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

68. 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

69. 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.

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

71. 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

72. 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.

73. 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.

74. 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 CIO file plan would appear as:

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

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

General Principles of Creating or Updating a File Plan

76. 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.

File Plan Maintenance

77. 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.

78. The completed file plan must incorporate a retention schedule recommendation for all files and also specify 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 Records Review Process ‘How to Guide’, available on the Information Portal.

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		Information 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		Equipment	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	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 "**D7**" denotes "Destroy 7 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.

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.

ELECTRONIC RECORD KEEPING IN A NTFS ENVIRONMENT

Background

1. This guide describes how units are to implement NTFS for records keeping in the absence of an ERMS

2. 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 The National Archives.

3. 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

4. The ISS Information Policy team 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 ISS Information Policy team.

What you should do

Electronic Records Management in a NTFS environment

5. 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.

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

7. 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.

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

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

    - 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.

    - 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; and a description of intended content.

    - 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.

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

Migrating from NTFS file structure to an ERMS

10. 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.

11. Electronic files held in a NTFS environment may possess very little by way of 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.

12. 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.

13. 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.

14. 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.

RECORD REVIEW PROCESS FOR DESK OFFICERS

BACKGROUND

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.
2. The MOD Departmental Record Officer has delegated the authority to business 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, and records that cease to have business value.
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 therefore important that the Information Manager (IMgr) ensures an effective system of review is maintained.
4. 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. Only staff at Band C2 (or equivalent) grade and higher are eligible to undertake these reviews.
5. While the majority of MOD's records will be destroyed at the end of their retention period some (approximately 5%) will be selected for permanent preservation at The National Archives (TNA). Examples of records which are likely to warrant permanent preservation are contained at Annex A.

WHAT YOU SHOULD DO

REVIEW OF ELECTRONIC FOLDERS

6. Electronic folders containing material not purely business administrative in 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 retention period.
7. 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.
8. Even if only one record is deemed to warrant a folder's retention period being extended while the other records retain 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.
9. 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.
10. 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 (see below) can be used to assist with this process and is available on the Defence Intranet.
11. 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 paper registered file accordingly.

REVIEW OF PAPER REGISTERED FILES

12. If a registered file contains material not purely business administrative in 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.
13. 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.

14. Even if only one enclosure is deemed to warrant a file's retention period being extended, while the other records retain no value at all, the whole file must be kept to ensure the information retains its integrity, as the "weeding" of enclosures from registered files is prohibited.
15. As already stated, 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, TNA requires MOD to select complete files for permanent preservation rather than extracts from files.
16. 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.
17. Once the Reviewing Officer has reviewed the file, the MOD Form 262F (parts 2 and 3) must be completed to advise their recommendation for the files disposal.
18. 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 paper registered file accordingly.

Annex A - Permanent Preservation of MOD Records

MOD Appraisal Report

1. The purpose of the **MOD's Appraisal Report** is to articulate to the public what records of MOD activity up until the present date they can reasonably expect to be transferred to The National Archives (TNA) in the future. Its basis is a high-level analysis of the structure, functions and activities of Defence, a determination of which of those structures, functions and activities generate records that are potentially worthy of permanent preservation, and evaluation of those records against TNA' selection policy. Underpinning this is an assumption that records are being managed appropriately in all areas Defence.

Examples of Records likely to warrant Permanent Preservation

2. These are likely to be documents or 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 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.

Annex B - Electronic Records Folder Review Form

1 FOLDER DESCRIPTION

Folder Name/Title:

Reference:

Part:

2 REVIEW DECISION

2a DESTROY IMMEDIATELY

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

2b RETAIN UNTIL YEAR (insert year) - **Retain for an extended period of time for business / administrative reasons.**

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):

Units **must** notify DBS KI of folders over 15 years old.

2c RECOMMEND TO DBS KI RECORDS AND REVIEW TO CONSIDER FOR PERMANENT PRESERVATION ☐

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

Units **must** ensure that the Meridio Permanent Preservation check box is checked.

3 REVIEWING OFFICER DETAILS

Name:

Role:	Rank/Grade:	Date:

4 FOR DBS KI USE ONLY

Date of 2nd Review:	Review Decision:	Reviewer:

(Revised 4/14)

RECORDS REVIEW PROCESS FOR INFORMATION MANAGEMENT STAFF

Background

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.

2. The MOD Departmental Record Officer (DRO) has delegated the authority to business 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.

What you should do

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 therefore important 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.

'What to Keep'

4. To help facilitate this the 'What to Keep' process is available to help business units ensure that they know what information they need to create and keep as records, how long to keep those records for, and how to put this into practice.

5. The 'What to Keep' process involves the following steps:

- Finding out what the business unit does and what information it holds.
- Deciding what needs to be kept, for how long, where and who is responsible for it and recording this in a What to Keep schedule.
- Devising processes to ensure that the schedules are implemented and kept up to date.
- Putting the processes and schedules into practice and monitor compliance. Business units will need to engage with their iHub to apply retention schedules and ownership to their records.

6. Further information is available here.

Retention Schedules

7. The IMgr is responsible for the creation and maintenance of the retention schedule, and co-ordinating the dissemination of electronic folders and paper registered files to be reviewed, to the relevant desk officer or subject matter expert (SME). This involves considering all existing electronic folders and registered files held by the unit and identifying which category each falls into. Categories are:

- Records which merit consideration by DBS KI for permanent preservation.
- Records which though not worthy of permanent preservation will need to be kept for an extended period for administrative purposes.
- Records which have only short term value and will not need to be retained for a lengthy period.

8. 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).

9. 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.

10. The desk officer or SME (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. Only staff at Band C2 (or equivalent) grade and higher are eligible to undertake these reviews

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

- Annex A provides guidance on how long to retain different types of records and examples of records that are likely to warrant permanent preservation.
- Annex B provides guidance on paper file plan management and the records lifecycle for both electronic and paper records.

THE REVIEW OF ELECTRONIC FOLDERS

12. 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.

13. All closed electronic folder parts must be reviewed within the allocated timescales, and the appropriate disposal action carried out.

14. 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.

15. 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 retention period. These folders can therefore be destroyed locally without seeking additional consent from the Reviewing Officer.

16. If it has been judged that a particular electronic 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.

17. Electronic folders containing material not purely business administrative in 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 retention period.

18. 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. Consideration must also be given to whether the material continues to merit its original security classification marking, or whether it should be downgraded.

19. 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.

20. Even if only one record is deemed to warrant a folder's retention period being extended while the other records retain 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.

21. 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.

22. 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 (see below) can be used to assist with this process and is available on the Defence Intranet.

23. 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 registered file accordingly.

24. **There is no requirement to maintain File Records Sheets (MOD Form 262A) or File Disposal Forms (MOD Form 262F) for wholly electronic folders, however there must be means of identifying when a folder part has been destroyed, so a method of producing disposal certificates and saving these on the system for 20 years must be devised**.

ACTIONS FOLLOWING THE REVIEW OF AN ELECTRONIC FOLDER

25. 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 DBS KI Records team; or destroy.

26. 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 (see below), into an appropriate electronic folder in the ERMS. This folder should have a retention schedule of 15 years applied to it. This form also acts as an audit trail for the iHub staff should there be a query on the location of the folder.

27. 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 ISS Information Policy team immediately for advice.

THE REVIEW OF PAPER REGISTERED FILES

28. When a registered file is closed, a MOD Form 262F **MUST** be raised and placed in the file on the right hand side (on top of the last enclosure). 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.

29. The IMgr must then consider whether the file is likely to be needed for administrative or historical purposes, as part of the initial review. Consideration must also be given to whether the material continues to merit its original security classification marking, or whether it should be downgraded.

30. The file minute sheet should also be checked to see whether the file contents include any items which, because of their bulk, could not be placed within the file. If it does, these items must be passed with the file to the relevant “owner” for review.

31. Where a registered file contains material of a local administrative nature, this usually indicates that its contents may not need to be kept beyond its stated retention period. If the file is then subsequently deemed to have no on-going administrative value, the IMgr should destroy it locally (in accordance with JSP 440). 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 15 years of its closure, permission must be sought, in writing and with a suitable justification, from the DRO to retain it further.

32. If the registered file contains material not purely business administrative in 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.

33. 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 (see Annex A).
  - 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 (see Annex A)
- Complete and sign Part 3 of the form and return it to the iHub.

34. Even if only one enclosure is deemed to warrant a file's retention period being extended, while the other records retain no value at all, the whole file must be kept to ensure the information retains its integrity, as the "weeding" of enclosures from registered files is prohibited.

35. As already stated, 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, TNA requires MOD to select complete files for permanent preservation rather than extracts from files.

36. 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.

37. Once the IMgr or the Reviewing Officer has reviewed the file, the MOD Form 262F (parts 2 and 3) must be completed to advise their recommendation for the files disposal.

38. 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 registered file accordingly.

The Review of Unregistered Records

39. 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 in JSP 441 Part 2 Guide Records 14 – When and Where to Forward Records to MOD Archives.

40. The "Record of Unregistered Records" 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

41. 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

42. 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.

43. 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.

44. Files which have on-going 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, the DRO must be advised in writing of any case in which the file is still required by the business unit for administrative purposes 15 years after closure.

45. 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 on-going retention of the file. Failure to do so may result in the file being destroyed by the DBS KI Records Review team.

46. 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 the ISS Information Policy team. Other departments should follow normal procedures.

Retention of Other Records

47. Unregistered records which merit consideration by the DBS KI Records Review team for permanent preservation must be forwarded to them within 15 years of their creation, in accordance with the instructions in How To Guide: When and where to forward records to MOD Archives.

48. Unregistered records required for administrative purposes may be retained by the business unit for up to 15 years after their creation. If the records have not been destroyed within 15 years permission must be sought, in writing and with a suitable justification, from the DRO to retain them.

49. 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.

Actions following the review of a paper registered file

50. 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 registered files held by the branch. (Note that closed files should not be stored alongside open files.)

Maintaining the MOD Form 262A and MOD Form 262F

51. 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.

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

53. Each MOD Form 262F must be retained for a period of not less than 20 years from the date of last enclosure (as recorded on the form).

54. 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 20 years following the insertion of the final MOD Form 262F. In every case, each MOD Form 262F must be retained for a period of at least 20 years from the date it replaces the MOD Form 262A.

55. 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.

56. When a registered file is destroyed by the business unit, the MOD Form 262F must be removed from the file and used to replace the MOD Form 262A in the MOD Form 262 binder. The MOD Form 262A must then be destroyed.

57. If the registered 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 duplicate copy of the MOD Form 262F, which is to be annotated to indicate that the file has been forwarded to the MOD Archives and then replaces the MOD Form 262A in the MOD Form 262 binder. The MOD Form 262A should then be destroyed.

58. When files are to be forwarded to the appropriate MOD Archives, care should be taken when completing Part 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.

Destruction of TOP SECRET Registered Files and Files Containing Codeword Material

59. All closed registered files containing TOP SECRET and/or codeword material are to be forwarded to the Sensitive Archive at HMNB Portsmouth, once no longer required for administrative reasons, even if the Registered File Disposal Form recommends that the file should be destroyed. They must not be destroyed locally.

60. 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.

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. The Historical Analysis team (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 15 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 15 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 1950s.
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 15 years.

Annex A – Appendix 1 - Permanent Preservation of MOD Records

MOD Appraisal Report

1. The purpose of the MOD's Appraisal Report is to articulate to the public what records of MOD activity up until the present date they can reasonably expect to be transferred to The National Archives (TNA) in the future. Its basis is a high-level analysis of the structure, functions and activities of Defence, a determination of which of those structures, functions and activities generate records that are potentially worthy of permanent preservation, and evaluation of those records against TNA' selection policy, to arrive at the answer that is set out in the Report. Underpinning this is an assumption that records are being managed appropriately in all areas Defence.

Examples of Records likely to warrant Permanent Preservation

2. These are likely to be documents or 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.

Annex A – Appendix 2 - Guidance on how long to keep records

Contracts

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

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.)

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

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

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.

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.

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.

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 seven years have been substituted in the advice given instead of the eighteen months and six years stated by NAO.

Cheques

Cheque book/butts for all accounts	7 years
Cancelled cheques	7 years
Dishonoured cheques	7 years
Fresh cheques	7 years
Paid cheques	7 years
Cheque stoppages	7 years
Cheque registers	7 years

Bank Details

Bank deposit books/slips/butts	7 years
Bank deposit summary sheets	7 years
Bank statements	7 years
Certificates of balance	7 years

Other Records

Expenditure sheets	7 years
Cash books	7 years
Petty cash receipts	7 years
Creditors' history records	7 years
Statements of outstanding accounts	7 years
Credit notes	7 years
Debit note books	7 years
Claims for payment	7 years
Purchase orders	7 years
Accounts payable (invoices)	7 years
Wages	7 years

Cost cards / costing records	7 years
Creditors' ledgers	7 years
Prime records for raising of charges	7 years
Year-end balances/published accounts	7 years
Postal records / books	7 years
VAT receipt books	7 years
Debts/overpayments/write-offs	7 years
Employee pay histories	7 years
Leaving staff	Keep last 3 years records for pension calculations
Salary rates register	As superseded
Stores inwards books	7 years
Stock control	7 years
Purchase orders	7 years
Travel warrants	7 years
Requisition records	7 years
All asset registers	7 years after last entry is disposed of

Building Records

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

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.

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

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.

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.

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.

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.

16. It is recommended that relevant records be kept for 40 to 60 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.

17. Arrangements for the reporting of health and safety, environmental incidents and accidents can be found in JSP 375 – Part 2 - Volume 1 – Chapter 16 – Accident/Incident Reporting and Investigation. MOD policy on the management and retention of health and safety records for all staff can be found in JSP 375 – Part 2 - Volume 1 – Chapter 39 – Retention of Records.

Personnel Files

18. 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).

19. 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.

20. 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 1 - Annex A) and then appropriately disposed of.

21. Medical records[3] should be kept as separate annual sub-sets of personal files. Armed services medical records can be made publicly available at 100 years from the date of the last entry on the record unless there are particular reasons not to do so.

Airworthiness Records

22. Details about Airworthiness records and how long these records should be retained can be found in Manual of Maintenance and Airworthiness Processes (MAP 01): Chapter 7.6 - Retention of Military Aviation Engineering Documentation.

Medical Records

23. Details about Medical records and how long these records should be retained can be found in JSP 950 - Lft 1-2-11, Annex A – Medical Policy.

Other types of records

24. Contact the Information Management Policy team for guidance on how long to keep other types of records.

Electronic folders

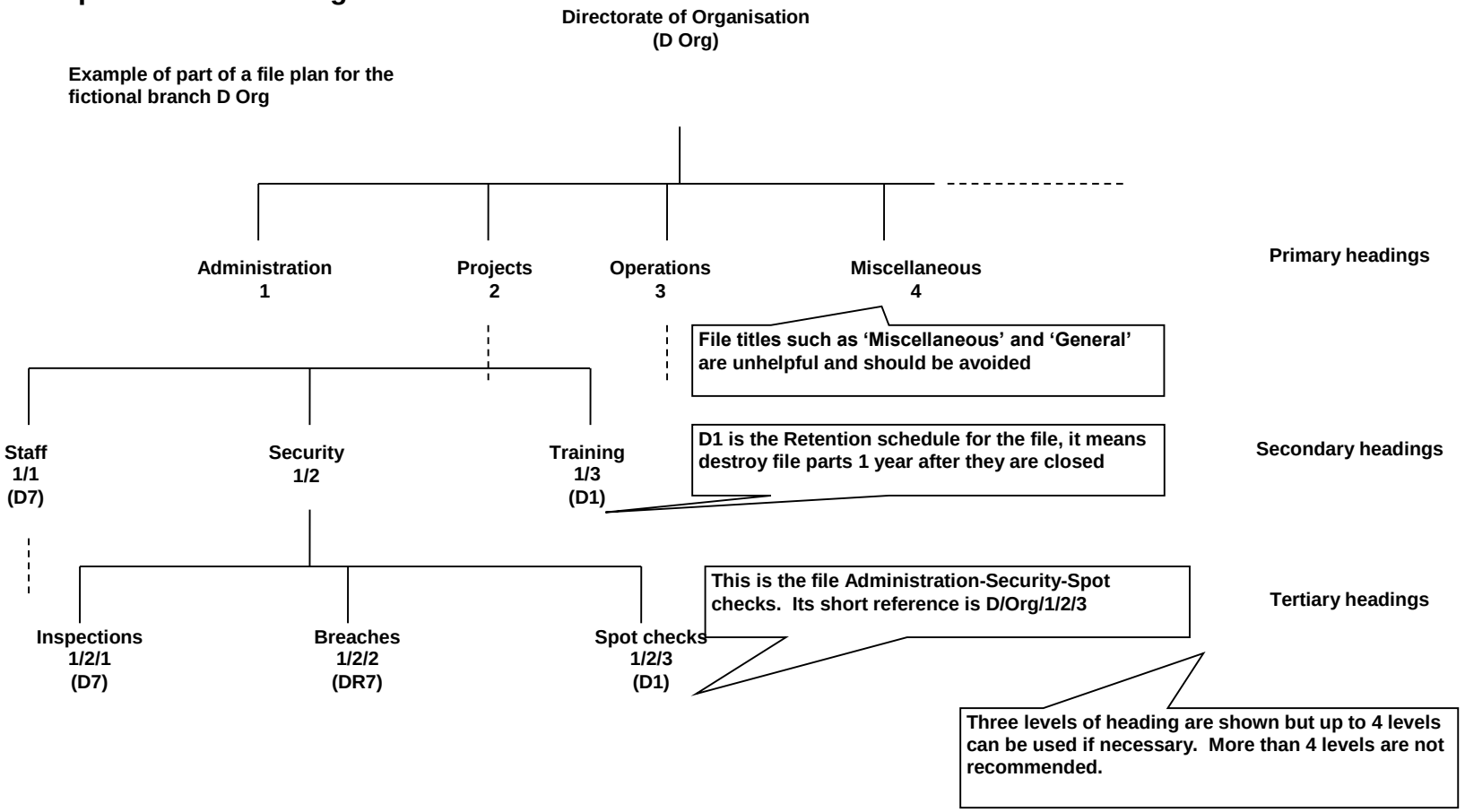
25. Retention schedules are an essential feature of all Electronic Records Management Systems (ERMS). They ensure that folders are reviewed (usually after a period of years) to determine the appropriate disposal action to be taken on that folder. Schedules can be assigned to the file plan and hierarchies of folders can inherit these as defaults from higher-level folders.

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 ISS Information Policy team (see contacts on the Information Portal).

27. It should be noted that in exceptional circumstances, for example where the defined retention schedule is too short, the ISS Information Policy team has the authority to override any local decisions.

[3] 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).

Annex B - Paper File Plan Management

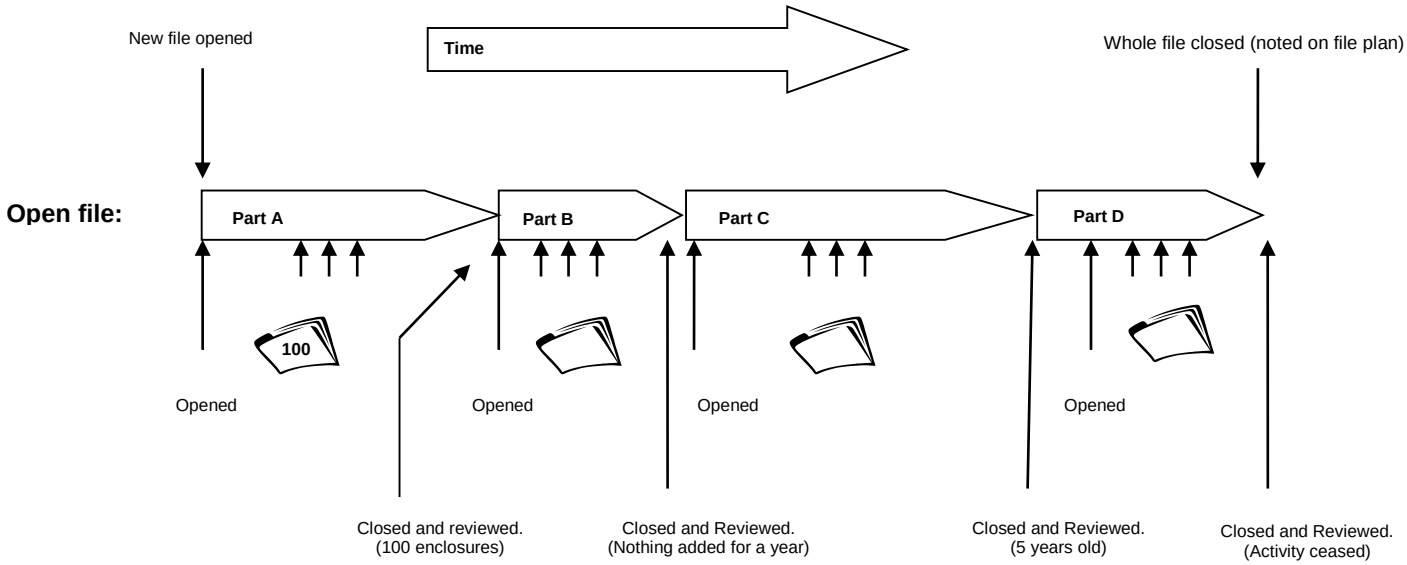


Notes:

- 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.
- Keep the file plan logical and simple.
- The Information Management Policy team can provide guidance on construction of file plans.

THE LIFE OF A PAPER REGISTERED FILE

Annex B

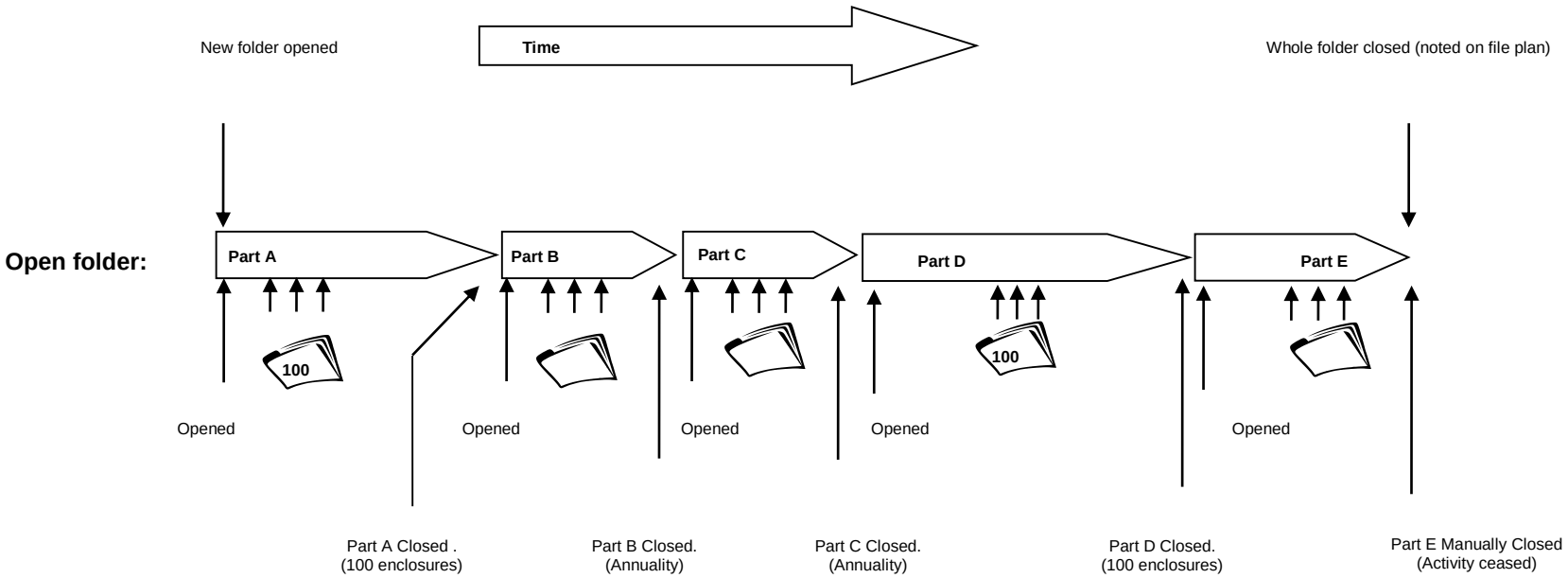


Notes:

- Here is the life-cycle of a typical paper 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), or nothing added for a year (Part B), or 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

Annex B



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.

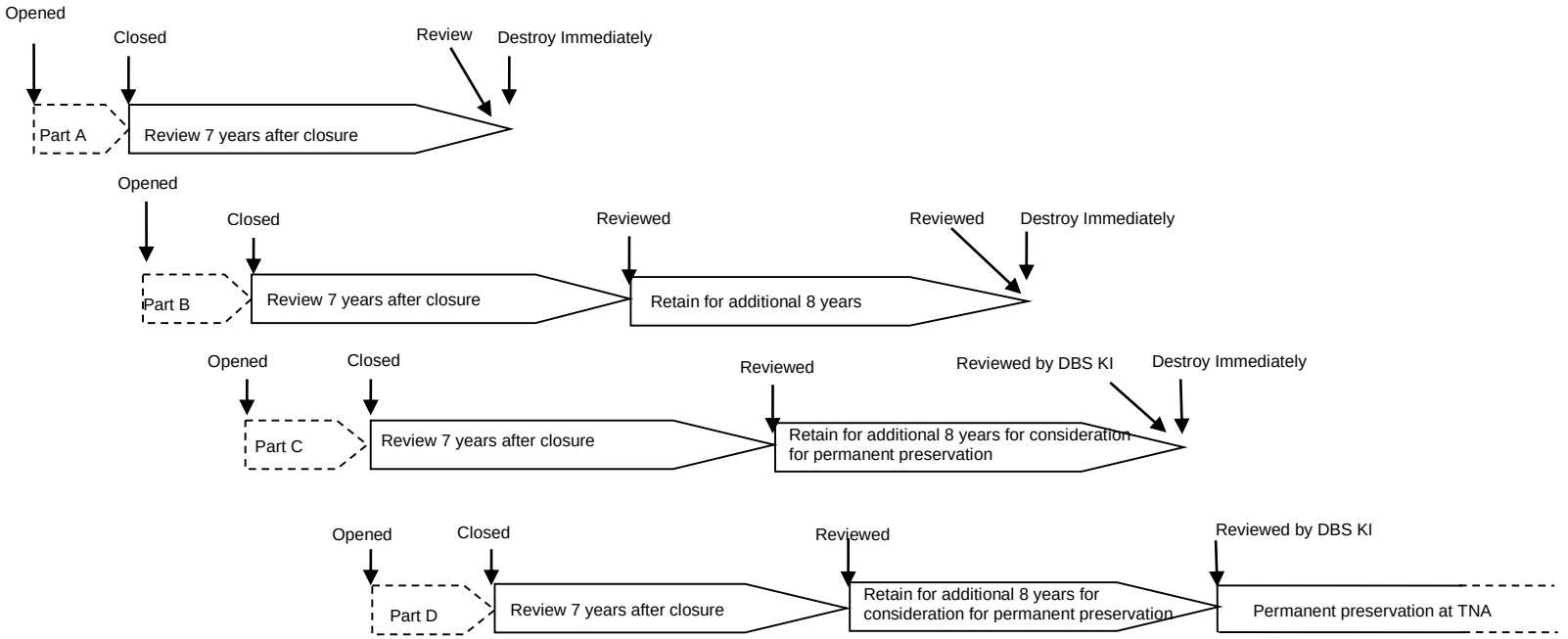
-Each new part is opened automatically when a specific criterion is reached and there is an enclosure to file on it. Note that this can result in zero enclosures in a part for a particular year.

-Parts are closed for several reasons: 100 enclosures (Parts A and D) and annuality (Parts B and C).

-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. Each Part will be reviewed when its associated retention period is reached.

THE LIFE OF A CLOSED ELECTRONIC FOLDER / REGISTERED FILE

Annex B



Notes:

-Here is the life-cycle of a closed electronic folder or registered file. The file's (as annotated on the MOD Form 262F) or folder's retention schedule states local review 7 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 purposes only.

-Part A is reviewed 7 years after its closure. The Reviewing Officer decides that it has no further value to the business unit or the MOD, and is not considered worthy of permanent preservation, so it is destroyed immediately by the iHub.

-Part B is reviewed 7 years after its closure by the Reviewing Officer who deems that it is still required for business purposes and so decides to keep the folder part for an additional 8 years. At the end of this additional period (retention schedule is changed to 15 years), it is deemed no longer required for business or other purposes and the file part is destroyed by the iHub.

-Part C is reviewed 7 years after its closure by the Reviewing Officer who decides that it may merit permanent preservation. The file part's retention schedule is then changed to 15 years. 15 years after its closure, the file part is reviewed by the DBS KI reviewer who decides that permanent preservation is not merited and marks it for immediate destruction.

-Part D is reviewed 7 years after its closure by the Reviewing Officer who decides that it may merit permanent preservation. The file part's retention schedule is then changed to 15 years. 15 years after its closure, the file part is reviewed by the DBS KI reviewer who agrees that permanent preservation is merited and arranges its transfer to TNA.

Annex C - Electronic Records Folder Review Form

1 **FOLDER DESCRIPTION**			
Folder Name/Title:			
Reference:			
Part:			
2 REVIEW DECISION			
2a DESTROY IMMEDIATELY			
Reason: Of no further administrative value and not worthy of permanent preservation.	☐		
2b RETAIN UNTIL YEAR (insert year) - **Retain for an extended period of time for business / administrative reasons.**			
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):			
Units **must** notify DBS KI of folders over 15 years old.			
2c RECOMMEND TO DBS KI RECORDS AND REVIEW TO CONSIDER FOR PERMANENT PRESERVATION	☐		
Of no further business /administrative value to MOD but has historic value. (Please specify historic value):			
Units **must** ensure that the Meridio Permanent Preservation check box is checked.			
3 REVIEWING OFFICER DETAILS			
Name:			
Role:		Rank/Grade:	Date:
4 FOR DBS KI USE ONLY			
Date of 2nd Review:	Review Decision:		Reviewer:

(Revised 4/14)

MANAGING VIDEO, FILMS AND PHOTOGRAPHS (INCLUDING OPERATIONAL AND AIR RECONNAISSANCE)

Introduction

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.

2. This guide 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

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.

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.

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

What you should do

The Imperial War Museum (IWM)

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).

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

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 guide, ‘video’ is to be used as the generic term to encompass motion pictures, including using digital techniques.

10. Where the term ‘film’ is used in this guide, it is to specifically distinguish a production that has been stored on cellulose material.

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 security classification marking.

12. Each year, any business unit responsible for making or sponsoring a video (for training video see paragraph below) in the preceding year is to forward details to the DBS KI Records Review team,

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.

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 here for contact details.

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 guide and must be followed.

When to transfer Video or Film Records

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 Records Review team for more details.

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.

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 Records Review team.

18. Once selection has been confirmed by the appropriate single Service Historical Branch or the DBS KI Records Review 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 Records Review 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 Records Review team will inform the recipient of selected material at the time of selection confirmation.

19. Material of a sensitive nature **MUST** be forwarded to the DBS KI Records Review 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 Records Review team (see Annex B).

What should be transferred?

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.

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.

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

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

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 guide):

- 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.

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

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.

27. Acetate film, produced from the 1930s to the 1970s, 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.

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

29. In all instances, contact the DBS KI Records Review team.

Where to send Non Digital Photographs

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

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

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

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 the Departmental Record Officer (DRO). If appropriate, the ISS Information Policy team (see contacts on the Information Portal) 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.

BDFL Contact Details

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-CustomerServices@mod.uk

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.

36. The DRO **MUST** be advised in writing of any case in which the material is still required by the business unit 15 years after its creation.

Annex A - Microform Records

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

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

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.

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.

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).

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.

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

Annex B - Sensitive Image Records

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).

2. Imagery selected for preservation but which still merit a security classification 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 Records Review team for storage in the appropriate archives.

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

Digital Material

4. Sensitive digital material being deposited to the DBS KI Records Review 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.

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 Records Review 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

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

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.

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

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

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 security classification marking applicable to the contents

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

Dispatch

12. Sensitive digital imagery and archive boxes containing sensitive non-digital imagery must be sent, in accordance with appropriate JSP 440 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

13. The DBS KI Records Review 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 Records Review team will contact the business unit regarding the queries that they may have on the material.

14. Once this validation process is complete the DBS KI Records Review 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 1 and 2 as appropriate) – **Do NOT send a copy of the listing to the IWM**.

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

Annex C - Minimum Standards for Digital Photographs

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.

Camera Guidance

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

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

- **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).

- 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.

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

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

Off-Line Storage Media

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[4]

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.

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.

Annex D - Transfer of Digital Material Selected for Permanent Preservation

Introduction

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

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

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

2. Adherence to this guide 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

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.

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

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[5] (subject to DPA restrictions), what, where, when and why (if possible).

[5] 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.

- Metadata should be entered in both the raw[6] and worked[7] 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[8], 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.
- Descriptions, acronyms, abbreviations, etc. must be intelligible and consistent and avoid using terms such as those below:
  - Mug shots
  - Interiors/exteriors
  - Royal visit
  - Funeral
  - SCC Group
  - X2 Portrait
  - PERRAS
  - Local children[9]
  - OC
  - The Boss
  - FNG
  - Ops
  - IRT

Complying with the MOD Metadata Standard

6. The MOD Metadata Standard (MMS) 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:

[6] 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.
[7] Worked image: A digital image that has been processed using imaging software. This is considered as being a digital print.
[8] 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.
[9] For their protection, the IWM will not accept images of children without the requisite completed consent form.

- 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 marking (for example OFFICIAL)
- Copyright (Normally 'Crown' for photographs taken by MOD staff)
- Whether the image has been processed (manipulated) and in what way.

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

Identifying the Type of Material Suitable for Archive

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.

9. Any images of adults and children that are to be transferred to the IWM must be accompanied with the requisite consent forms. DIN 2012DIN05-006 (Consent Form for Defence Imagery) directs the Defence-wide use of the MOD Imagery Consent Form in compliance with the MOD's legal obligations, where the consent of persons who feature in imagery (photographs, audio/videos, films) is required prior to publication for all purposes stated on the form. Where there are subjects under 18 years of age, particular care must be taken for such consent to be secured before photography/recording takes place.

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.

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)

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

Transfer of Digital Material

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.

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 Defence Communications (DDC).

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

Packaging Information

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.

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.

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.

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 1 for digital images or Annex D – Appendix 2 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 the DBS KI Records Review team.
- (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[10] 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 1 and 2) 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

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

[10] 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.

Imperial War Museum
Lambeth Road, London, SE1 6HZ

Tel: [redacted]

E-mail: [redacted]

Where to Send Digital Photographs

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

22. DDC 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. DDC 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.

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

Directorate of Defence Communications
Defence Imagery
Level 1, Zone C, Desk 2
MOD Main Building,
Whitehall, London
SW1A 2HB

Tel: 0207 218 6997

Email: admin@photos.mod.uk

Validation of Deposited Material

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.

25. Once this validation process is complete the IWM will send an email confirming the successful transfer and validation of the material to the named civilian email address identified in the declaration form (See Appendices 1 and 2 as appropriate).

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

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

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

Title / TASK NUMBER	Production Date	Subject Matter	Security Classification	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.: [redacted]
Email: DBSKI-RecordsReview14@mod.uk	Email: [redacted]

Annex D – Appendix 2

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

Title / TASK NUMBER	Production Date	Duration	Subject Matter	Security Classification	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.: [redacted]
E-mail: DBSKI-RecordsReview14@mod.uk	E-mail: [redacted]

Annex E - Transfer of Non Digital Material Selected for Permanent Preservation

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: [redacted]

  E-mail: [redacted]

- **For Photographs**:

  Head of Collections Management
  Photograph Archive
  Imperial War Museum
  Lambeth Road, London, SE1 6HZ

  Tel: [redacted]

  E-mail: [redacted]

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

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.

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

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 1 and 2 as appropriate.
- The review decision for each item (i.e. deposit or presentation).
- The institution selected to receive it.

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

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.

8. The archive box must be sent, in accordance with appropriate JSP 440 procedures to the IWM.

Validation

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.

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.

HANDLING TOP SECRET, STRAP AND CODEWORD RECORDS

Background

1. All MOD personnel are required to share information responsibly and sensibly. JSP 440 - 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.

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 for more details. Failure to adhere to these policies may lead to disciplinary proceedings.

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.

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 for more details.

5. The definition of the TOP SECRET security classification, and instructions for maintaining, sending and receiving such material, are contained within JSP 440.

Specific Policy

6. Intelligence and Security Agency End Product[11] **MUST NOT** be declared as a MOD record, and will be retained by the originating Agency in accordance with their records management policies.

What you should do

Electronic Records

7. Unless using a Departmental Record Officer (DRO) approved ERMS, 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 JSP 441 Part 2 Guide Records 02, Paper Records Management Procedures, unless alternative arrangements have been agreed with the ISS Information Policy team.

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

9. DRO approved ERMS' handling TOP SECRET material, are to comply with the requirements as laid down in JSP 441 Part 2 Guide Records 01, Electronic Records Management Procedures. In addition 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 15 years or older.

Paper and Non Digital Imagery Records

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 JSP 441 Part 2 Guide Records 14, Where and When to Forward Records to MOD Archives.

11. Non digital imagery selected for preservation, but which still merits a TOP SECRET security classification marking, **MUST** be forwarded to the DBS KI Records Review team for storage in

[11] 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).

the appropriate archives. There is no requirement to forward foreign owned or Agency imagery material to the MOD Archives.

12. TOP SECRET imagery **MUST NOT** be forwarded 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 procedures, to the DBS KI Records Review team. See JSP 441 Part 2 Guide Records 06, Handling Video, Film and Photographs.

Review and Disposal of Records

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

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.

15. The DBS KI Records Review team is then to be given access to the material together with the reviewing officer's recommendation.

16. Where the business unit has a requirement to retain records locally beyond the 20-year limit set by the Public Records Act, the MOD must submit an application through the ISS Information Policy team to the Lord Chancellor's Advisory Council.

17. Business units **MUST NOT** destroy TOP SECRET material. **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.

18. The review and disposal of the file will be carried out by the DBS KI Records Review team in accordance with JSP 440.

MANAGING RECORDS WHEN UNITS CLOSE

Background

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

What you should do

2. Prior to its closure, the unit iHub must make arrangements for electronic folders and registered files to be reviewed by suitable reviewing officers. Except for material classified TOP SECRET, those electronic folders and registered files no longer required because they are no longer required for business use, have passed their retention periods, and have no historic value, should be destroyed locally – in accordance with JSP 440.

3. Units **MUST NOT** destroy TOP SECRET material. All closed registered files containing TOP SECRET, STRAP and/or codeword material are to be forwarded to the Sensitive Archives in Portsmouth, even if the Registered File Disposal Form (MOD Form 262F) recommends that the file should be destroyed. The review and disposal of these registered files will be carried out by the DBS Knowledge and Information Services Records and Review team in accordance with JSP 440.

Electronic Records

4. The custodianship of those electronic folders that need to be retained for business purposes should be transferred to the successor or parent unit and funding provision planned for, in those situations where electronic records are to be transferred from one system to another.

Physical Records – Registered Files

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

- Sent to the MOD Main Archives for material classified up to SECRET or the MOD Sensitive Archives for material classified above SECRET.
- Transferred to the successor or parent unit, if still required for business use.

6. Records which are not to be transferred to another unit, but nonetheless appear to warrant permanent preservation or have long term administrative value, should be forwarded to the appropriate MOD Archive.

7. All copies of MOD Form 262F for material sent to Archives **MUST** be passed to the successor or parent business unit. If there is no suitable unit they must be sent to the relevant MOD Archive.

8. All 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 DBS Knowledge and Information Services Contract Management Team is to be notified. The Contract Management Team (CMT) will provide assistance with the planning and costing of the movement of registered files that are destined for the MOD Main Archive. If you plan to send a large quantity of paper records to the MOD Main Archive, contact the Contract Management Team advising the type and quantity of records involved. This will ensure that suitable provision can be made for their arrival. The Contract Management Team can be contacted by:

Email: DBSKI-RecordsCMTMgr@mod.uk

Telephone: (9)4240 5701 / 01869 259701

Physical Records – Unregistered Files

9. 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.

TRANSFER OF RECORDS TO OTHER BUSINESS UNIT

Background

1. The need may arise to transfer paper registered file(s) or electronic files and folder(s) 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.

2. This guide contains instructions for both electronic and paper records. Guidance on transferring MOD records to other government departments is contained in JSP 441 Part 2 Guide, Records 10, Machinery of Government Change/Transfer of information to Other Government Departments.

What you should do

3. The first thing to do is review the physical registered files and electronic folders. Those files which are no longer required, i.e. they have passed their retention periods, are no longer required for business use and have no historic value, should be destroyed (in accordance with JSP 440: The Defence Manual of Security).

Electronic Records

4. When such a need arises the ISS Information Policy team must be advised in writing before action is taken (see contacts on the Information Portal).

5. 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.

6. Electronic folders must not be renamed and 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.

7. The "exporting" business unit must notify the ISS Information Policy team 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.

Paper registered files

8. The first thing to do is review the files. Those files which are no longer required, i.e. they have passed their retention periods, are no longer required for business use and have no historic value, should be destroyed (in accordance with JSP 440: The Defence Manual of Security).

9. Once reviewed, the files (along with their MOD Form 262Fs) should be transferred to the successor business unit. If space is limited or they are not required for immediate business use they may be sent to the relevant MOD Archives.

10. It may be possible to retain the existing file numbers and amend the business unit title on the file covers. The Departmental Record Officer should be advised in writing (via this address) if such action is taken.

11. 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.

12. 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).

13. 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.

14. 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 the DRO of the transfer.

15. 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.

MACHINERY OF GOVERNMENT CHANGE AND TRANSFER OF INFORMATION TO OTHER GOVERNMENT DEPARTMENTS

Background

1. Where some or all functions of a unit are to be transferred between Ministers, either between Ministers in charge of Departments or other Cabinet Ministers, or between a Minister and a non-Departmental public body (NDPB) as a result of a Machinery of Government (MoG) change, the unit's information, records and knowledge needs to be properly transferred to the OGD in an orderly manner.

What you should do

2. All units liable to be affected by a MoG change should carry out advanced planning so that the transfer of records, information and knowledge can be achieved efficiently. Units affected by a MoG change must have a clear understanding of their roles and responsibilities and will need to work closely with MOD's Departmental Record Officer (DRO) to achieve an effective transfer of their paper and electronic records, as well as informally held information and knowledge.

3. To facilitate this transfer, the unit Information Manager (IMgr) is to arrange for a transfer agreement, finalising the transfer of records from the unit to the OGD, to be agreed and signed off by the DRO prior to transition day.

4. To obtain the details needed to populate the transfer agreement, the unit must perform an assessment of its record holdings, prior to transition day, to determine which records are going to remain in the MOD and which are likely to be required by the OGD. This assessment should include all the unit's records irrespective of format. During this assessment it will be necessary to identify, in each case:

- Not just the potential long-term value of the material for the administrative purposes of the MOD but also whether the information contained in the records warrants consideration for permanent preservation. The types of record likely to have long-term administrative/historical value can be found in the Records Management Portal.

- Those records thought to have no value to the OGD but that must be retained by MOD (either the unit's remnant body or the MOD Archives).

- Those records thought to have value to the OGD. These should be entered in a register, which would subsequently be the subject of adjudication by the MOD. This adjudication will be recorded in the transfer agreement.

- Those records, which must be retained by MOD but will also be needed by the OGD for reasons of business continuity, both in the context of general reference and in relation to specific work in hand. The unit's remnant body is to arrange for copies to be provided to the OGD. This also is to be recorded in the transfer agreement.

5. Details of the kinds of records that, at the very least, are of value to the MOD and therefore must not be destroyed locally can be found in JSP 441 Part 1 (Records Management Rules). If such records are held and do not form part of any subsequent OGD exercise justifying continued retention on ongoing business grounds, these should be retained by the unit's remnant body or forwarded to the MOD Main Archive at Swadlincote or (for TOP SECRET) Portsmouth.

6. An agreement between the MOD and OGD DRO must be reached about the transfer of records older than 15 years old. Where it is decided not to transfer these records to the OGD, the unit must pass them to the appropriate MOD Archives, where staff will then carry out the process of selection and transfer to The National Archives. Transferring only the records under 15 years old would ensure that the OGD does not inherit a review backlog.

Paper/Physical Records

7. The remnant unit files that are not required for current business purposes should be stored in the archives in Swadlincote or Portsmouth. These will then be reviewed in accordance with MOD procedures.

8. Before sending any large volumes of files to Swadlincote (or Portsmouth), the unit must contact the DBS Contract Management Team who will arrange for a special project to be set up. The DBS Contract Management Team must be closely involved in the planning of the transfer of files to TNT and discussions with TNT should not take place without this team's knowledge.

9. The cost of sending files to TNT and their indexing should be met by the unit transfer project. The DRO will not meet these costs as this is not day to day business. Additionally, where the unit does not currently use the MOD Main Archive, all the costs associated with the unit's holdings that are required for business purposes in the MOD Main Archive will fall to the unit, including any review or collation reallocation activities.

10. To help compile the transfer agreement:

- An inventory of paper files must be created to establish how many files are likely to be placed with TNT (this will allow planning and costing to take place) and how many fall into the Secret and below category and those requiring special handling (e.g. Top Secret). Any files falling into the latter category must not be sent to TNT but to the Sensitive Archive in Portsmouth. The DBS Knowledge and Information Records Review team must be advised of numbers to be submitted, etc. Time frames for when this archiving activity will happen should also be identified.

- The unit should request from TNT a breakdown of the numbers of files (and their security classification) currently held on the unit's behalf that will transfer to the OGD.

- The unit will need to provide a breakdown of the files currently held locally (not at Swadlincote), how many would be archived and destroyed, and how many would need to be transferred to the OGD.

11. Before sending records to TNT they should be reviewed by desk officers however, if in any doubt, retain the file rather than destroy it locally.

12. Following transition day, the OGD must not send any further material to MOD archives.

13. A sponsor should be established within the unit's remnant body so that if the OGD requires access to other files held by MOD, the sponsor can check, approve or otherwise and request them from TNT or the DBS Knowledge and Information Records Review team on their behalf.

14. The unit IMgr should contact the DBS Knowledge and Information Records Review team if further advice or guidance relating to the handling, transfer and archiving of physical records is needed.

Electronic Records

15. All electronic records, held in the official electronic records management system (ERMS), and which remain within the MOD, must be kept online with the unit's remnant body.

16. For those records "held" by individuals and which are not stored in an ERMS, it is the individuals' responsibility to assess which of their records should be included in the transfer, taking account of business needs and permanent preservation aspects.

17. Any electronic records that are to be transferred to the OGD must be transferred in a secure manner in accordance with JSP 440.

18. The unit IMgr should contact the DRO (via this address) if further advice or guidance is needed relating to the handling, transfer and archive of electronic records.

Personnel Files

19. The future of personnel files for those unit staff leaving MOD employment should be discussed with DBS Civilian Human Resources.

Freedom of Information (FOI)

20. FOI must be considered with regard to a focal point being established within the unit's remnant body for the unit files stored with TNT, as the DBS Knowledge and Information Records Review team will not undertake the FOI role for those files.

21. The unit iMgr should contact the DRO if further advice or guidance is needed.

Transfer Agreement

22. A transfer agreement must be raised by the unit, in consultation with the DRO. The transfer agreement finalises the transfer of records from the MOD to the OGD and must include a list of all records transferred. This agreement must be signed off by the DRO for both the MOD and the OGD. The agreement will include:

- A detailed list of files (including those held in the MOD Archive at Swadlincote) currently held by the unit that will be transferred to the OGD.
- A list of Vital Records (e.g. unique documents such as Memoranda of Understanding and Letters of Agreement) to be transferred to the OGD.

More Information

23. A transfer agreement template can be found at JSP 441 Part 2 Guide Records 12.

24. 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 the DRO. This guidance is also useful for those personnel who are involved in preparing their business units for closure.

UNIT TRANSFER TO A PRIVATE SECTOR BODY

Background

1. Where some or all tasks of a unit are to be transferred to a Private Sector Body (PSB), for example its services are contracted out or part or all of the unit is privatised, then the unit IMgr is to arrange for a transfer agreement, finalising the transfer of records from the unit to the PSB, to be agreed and signed off by the Departmental Records Officer (DRO) prior to vesting day.

What you should do

2. To obtain the details needed to populate the transfer agreement, the unit must perform an assessment of its record holdings, prior to vesting day, to determine which records are going to remain in the MOD and which are likely to be required for the PSB. This assessment should include all the unit's records irrespective of format. During this assessment it will be necessary to identify, in each case:

    - Not just the potential long-term value of the material for the administrative purposes of the MOD but also whether the information contained in the records warrants consideration for permanent preservation. The types of record likely to have long-term administrative/historical value can be found in JSP 441 Part 1 (section on Records Management Rules).

    - Those records thought to have no value to the PSB but that must be retained by MOD (either the unit remnant body or the Archives).

    - Those records thought to have value to the PSB. These should be entered in a register, which would subsequently be the subject of adjudication by the MOD. This adjudication will be recorded in the transfer agreement. Records older than 15 years old must not be transferred to the PSB, but may be provided to the PSB as a loan.

    - Those records, which must be retained by MOD but will also be needed by the PSB for reasons of business continuity, both in the context of general reference and in relation to specific work in hand. The unit remnant body is to agree to their temporary retention by the PSB as a loan. These loan items must be recorded in the transfer agreement.

3. Details of the kinds of records that, at the very least, are of value to the MOD and therefore must not be destroyed locally can be found in the Records Management Portal. If such records are held and do not form part of any subsequent PSB exercise justifying continued retention on on-going business grounds, these should be retained by the unit remnant body or forwarded to the MOD Main Archive at Swadlincote or (for TOP SECRET) Portsmouth.

Gifting/Transfer

4. All the unit records are MOD property and must be handled accordingly. The unit IMgr must ensure that records are not passed to local museums or other similar institutions. It is possible that some records might fall into the category of interesting but not worthy of permanent preservation and not required by MOD or the PSB. Through the proper channels these papers may be gifted to museums etc. This will only take place after formal review and consultation with The National Archives (TNA).

5. Where records are identified as no longer required by MOD but needed by the PSB, or where the PSB has, for example identified volumes of technical records, no longer required by MOD that it wants to retain indefinitely as reference material, these can be formally presented to the PSB. This 'gift' has to be agreed by TNA as on presentation the ownership of the records transfers from MOD to the PSB. These presented records thus become PSB property and lose their status as public records and are no longer subject to the provisions of the Public Records Acts 1958 & 1967. The PSB may retain them for as long as it wishes and may destroy them when of no further use.

6. A register of the records to be presented to the PSB is to be detailed in the transfer agreement.

7. Records created by the PSB after vesting date, are not public records.

8. If and when these records cease to be of business value to the PSB, it may feel that some should be preserved in an historic archive. If so, advice should be sought from the MOD's DRO.

Loan

9. There may be records that MOD still requires, but which are also needed by the PSB, for example material to be retained by the PSB in relation to specific and continuing MOD support activities. Should this be the case, MOD can agree to "loan" the identified records for a set period of time. These records would still be considered as public records and the PSB would be responsible for maintaining them to MOD standards.

10. The loan period should not exceed ten years and should the PSB cease trading or the need to hold the documents expire before the ten years has lapsed, the records must be returned to the MOD.

11. The PSB must hold these loaned records in secure facilities and not transfer them to any third party without MOD approval.

12. The PSB must not destroy these loaned records without MOD approval.

13. This process must be outlined in the transfer agreement.

Paper/Physical Records

14. The remnant unit files that are not required for current business purposes should be stored in the archives in Swadlincote or Portsmouth. These will then be reviewed in accordance with MOD procedures.

15. Before sending any large volumes of files to Swadlincote (or Portsmouth), the unit must contact the DBS Contract Management Team who will arrange for a special project to be set up. The DBS Contract Management Team must be closely involved in the planning of the transfer of files to TNT and discussions with TNT should not take place without this team's knowledge.

16. The cost of sending files to TNT and their indexing should be met by the unit transfer project. The DRO will not meet these costs as this is not day to day business. Additionally, where the unit does not currently use the MOD Main Archive, all the costs associated with the unit's holdings that are required for business purposes in the MOD Main Archive will fall to the unit, including any review or collation reallocation activities.

17. To help compile the transfer agreement:

    - An inventory of paper files must be created to establish how many files are likely to be placed with TNT (this will allow planning and costing to take place) and how many fall into the Secret and below category and those requiring special handling (e.g. Top Secret). Any files falling into the latter category must not be sent to TNT but to the Sensitive Archive in Portsmouth. The DBS Knowledge and Information Records Review team must be advised of numbers to be submitted, etc. Time frames for when this archiving activity will happen should also be identified.

    - The unit should request from TNT a breakdown of the numbers of files (and their security classification) currently held on the unit's behalf that will transfer to the PSB.

    - The unit will need to provide a breakdown of the files currently held locally (not at Swadlincote), how many would be archived and destroyed, and how many would need to be transferred to the PSB.

18. Before sending records to TNT they should be reviewed by desk officers however, if in any doubt, retain the file rather than destroy it locally.

19. Following vesting day, the PSB must not send any further material to MOD archives.

20. A sponsor should be established within the unit remnant body so that if the PSB requires access to other files held by MOD, the sponsor can check, approve or otherwise and request them from TNT or the DBS Knowledge and Information Records Review team on their behalf.

The sponsor is also responsible for checking that the PSB is maintaining any retained MOD files in accordance with requirements.

21. The unit IMgr should contact the DBS Knowledge and Information Records Review team if further advice or guidance relating to the handling, transfer and archiving of physical records is needed.

Electronic Records

22. All electronic records, held in the formal electronic records management system (ERMS), and which remain within the MOD, must be kept online with the unit remnant body.

23. For those records "held" by individuals and which are not stored in an ERMS, it is the individuals' responsibility to assess which of their records should be included in the transfer, taking account of business needs and permanent preservation aspects.

24. Any electronic records that are to be transferred to the PSB must be transferred in a secure manner in accordance with JSP 440.

25. The unit IMgr should contact the DRO, if further advice or guidance is needed relating to the handling, transfer and archive of electronic records.

Personnel Files

26. The future of personnel files for those unit staff leaving MOD employment should be discussed with DBS Civilian Human Resources.

Freedom of Information (FOI)

27. FOI must be considered with regard to a focal point being established within the unit remnant body for the unit files stored with TNT, as the DBS Knowledge and Information Records Review team will not undertake the FOI role for those files. The PSB must also be aware of FOI in relation to the retained/loaned (but not "presented") files they may hold.

28. The unit IMgr should contact the DRO if further advice or guidance is needed.

Transfer Agreement

29. A transfer agreement must be raised by the unit, in consultation with the DRO. The transfer agreement finalises the transfer of records from the MOD to the PSB and must include a list of all records transferred. This agreement must be signed off by the PSB records officer and the DRO. The agreement will include:

- A detailed list of files (including those held in the MOD Archive at Swadlincote) currently held by the unit that will be transferred to the PSB.
- A detailed list of those records that will be provided to the PSB on temporary retention, as a loan.
- A list of Vital Records (e.g. unique documents such as Memoranda of Understanding and Letters of Agreement) to be transferred to the PSB.

More Information

30. A transfer agreement template can be found at JSP 441 Part 2 Guide Records 12.

31. More information can be found in The National Archives document: "What to do if your public body is being privatised?"

TRANSFER AGREEMENT TEMPLATE

Transfer Agreement

Transfer of

<Name Of Transferring MOD Unit>

Records And Electronic Databases to the

<Name Of Receiving OGD or Private Sector Body>

on <Date>

All records and databases detailed in the attached annexes are to be transferred from <**NAME OF TRANSFERRING MOD UNIT**> to the <**NAME OF RECEIVING ODG** or Private Sector Body**>** to facilitate the transfer of <**NAME OF FUNCTION**> to this body.

Paper records transferred: See Annex A

Electronic records transferred: See Annex B

Electronic databases transferred: See Annex C

TRANSFERRING MOD Departmental Record Officer (DRO):

I confirm that records listed in Annexes A-C have been transferred to the receiving Department

Name:

Position:

Signature: **Date:**

RECEIVING OGD DRO or **Private Sector Body Records Officer:**

I confirm that I have received the records listed in annexes A-C

Name:

Position:

Signature: **Date:**

Annexes:

Annex A
List of paper records to be transferred

Annex B
List of electronic records to be transferred (folders or groups of records rather than individual documents)

Annex C
List of databases to be transferred

Annex D
List of vital records to be transferred

Annex E
List of records to be 'presented' to Private Sector Body

Annex F
List of records to be 'loaned' to Private Sector Body

Annex G
List of missing paper files and any electronic records that could not be transferred

Annex H
Procedures for completing the transfer agreement

1. The transferring MOD Unit IMgr should complete the form and on transferring the records arrange for the MOD DRO to sign, date and send the form to the receiving organisation.
2. The receiving organisation should carry out a check of the records it has received before finally signing and dating the transfer agreement.
3. The receiving organisation should keep the completed form and pass a copy to the transferring MOD Unit and MOD DRO.
4. The transferring MOD unit should also ensure that where appropriate: retention/disposal information, appraisal information, FOI issues, card indexes and other finding aids, 0 files, prefix bibles, information relating to databases, printed guidance or manuals relevant to the function or to databases, paper files relating to databases are also passed to the receiving organisation.

ORDERING FORMS FROM FORMS AND PUBLICATIONS COMMODITY MANAGEMENT

Background

1. The Departmental Record Officer, 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 174A	Temporary Enclosure Jacket (TEJ) – TOP SECRET
MOD 174B	Temporary Enclosure Jacket (TEJ) – SECRET
MOD 174D	Temporary Enclosure Jacket (TEJ) – OFFICIAL
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 329D	Registered File Cover – OFFICIAL
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

What you should do

2. To order more forms, 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.

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

WHEN AND WHERE TO FORWARD RECORDS TO MOD ARCHIVES

Background

1. Records held by units should normally be forwarded to the MOD Main Archives run by TNT Archive Services, or the MOD Sensitive Archives within 5 years of their closure unless the 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 15 years of their closure unless prior written authority has been obtained from the Departmental Record Officer to retain them.

2. Records may also be forwarded to the archives as part of a unit closure process or as a result of a Machinery of Government change.

What you should do

3. Ensure that all records that have potential historic or long-term value are transferred to the relevant MOD Archives.

Where to send records to MOD Archives

4. In addition to the MOD Main and Sensitive Archives, there are other destinations for records being forwarded to MOD Archives. The appropriate destination is determined by the types of record generated by units and the appropriate location to send these records are listed in the following table.

<table>
<tr><th>Originator</th><th>Type of Record</th><th>Send to:</th></tr>
<tr><td>All</td><td>TOP SECRET and Codeword registered files and files containing Atomic and Nuclear records.</td><td>MOD Sensitive Archives
1st Floor, Building 2/003
Gloucester Road
HM Naval Base
Portsmouth
PO1 3NH
9380 25252</td></tr>
<tr><td>All</td><td>Registered files (other than TOP SECRET and Codeword file and files containing Atomic and Nuclear records).</td><td rowspan="2">TNT Archive Services
Tetron Point
William Nadin Way
Swadlincote
Derbyshire, DE11 0BB
Tel: 0845 601 0610
Fax: 01827 312515
pangovarchive@tnt.co.uk</td></tr>
<tr><td>All</td><td>Civilian personnel records.</td></tr>
<tr><td>All</td><td>Service personnel records.</td><td rowspan="2">Refer to single-Service guidance</td></tr>
<tr><td>Single Services</td><td>Key Operational Records.</td></tr>
<tr><td>All</td><td>All other records.</td><td>TNT Archive Services
Tetron Point
William Nadin Way
Swadlincote
Derbyshire, DE11 0BB
Tel: 0845 601 0610
Fax: 01827 312515
pangovarchive@tnt.co.uk</td></tr>
</table>

More Information

5. For further details see JSP 441 Part 2 Guides:

- Records 08 - Managing records when units close.
- Records 10 - Machinery of Government Change.
- Records 16 - Using the MOD Main Archives.
- Records 17 - Using the MOD Sensitive Archives.

TRANSFER OF MOD RECORDS WITH HISTORIC VALUE TO THE NATIONAL ARCHIVES

Background

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

What you should do

2. Ensure that **all** records that have potential historic value are transferred to the relevant **MOD Archives**.

Transfer of Selected Records to The National Archives

3. Records which are selected as worthy of permanent preservation are prepared for transfer to 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.

4. The Public Records Act, as amended by the Constitutional Reform and Governance Act 2010, makes provision for the continued closure of some records which are identified as being too sensitive to release after 20 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 the Departmental Records Officer (DRO) within 15 years of their creation/closure. Any unit holding records in this category should write to the DRO who will provide specific guidance.

Presentation (Gifting) of Records to Museums or other Institutions

5. MOD records must not be passed to museums or other similar institutions without the consent of the DRO. The decision to gift records that have not been selected for permanent preservation to another institution is made by the DRO in consultation with TNA and these offers require the final approval of the Lord Chancellor.

6. 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 the DRO. If appropriate, the DRO in consultation with TNA will seek approval from the Lord Chancellor in accordance with Section 3(6) of the Public Records Act 1958, for the formal Presentation of the material to the relevant museum or institution.

USING THE MOD MAIN ARCHIVES

General Information

1. The following procedures should be complied with when sending files to the MOD Main Archives at Swadlincote. General guidance is shown below but for full details, including for withdrawing files from the MOD Main Archives, please refer to the TNT Archive Services Guide that can be found on the Records Management Portal on the Defence Intranet.

2. **TOP SECRET** material or material requiring special handling, **MUST NOT** be sent to the MOD Main Archives at Swadlincote – This material **MUST** be sent to the MOD Sensitive Archives at HMNB Portsmouth.

New Business Forms

3. TNT Archive Services new business forms **MUST** be used with correct collation codes[12] to identify the originating unit and the record type being submitted to the MOD Main Archives. Two copies should be sent with the records, one of which will be returned by TNT Archive Services to acknowledge receipt.

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

Registered Files

5. Each registered 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 (the disposal recommendation) and destruction date – where applicable (Part 2 of the form); a branch stamp including full address/telephone number (at Part 3); and a signature of the reviewing officer of the correct grade (Band C2/Service equivalent or above). Files lacking these details will **NOT** be accepted by TNT Archive Services and will be returned to sender.

6. File titles/numbers on covers are to be clearly legible.

7. Documents **MUST** be in Registered File covers – not Temporary Enclosure Jackets, branch folders, or bundles of loose papers, etc.

8. A copy of the MOD Form 262F **MUST** be retained by the unit as a record of all files archived at the MOD Main Archives.

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

10. Bundles of files should be clearly labelled and strapped or tied together.

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

12. Records which are due to be destroyed imminently should not be sent to the MOD Main Archives.

Unregistered Records

13. 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.

14. 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 using the new business forms. The highest security classification marking of the enclosed material, the year of its origin and the reason that its permanent preservation is being recommended must also be indicated. TNT Archive Services will keep one copy of the new business form and return the other as a receipt.

15. As unregistered records are stored in a different section of the archive, the correct collation code must be identified on the new business form and unregistered records **MUST NOT** be mixed with registered files.

Bundles

16. Bundles of registered files or other material must be clearly labelled and strapped together with 2 copies of a list of contents.

Receipts

[12] The collation codes can be found on the Records Management Portal on the Defence Intranet

17. A MOD Form 24 (Receipt) for each SECRET document, file, bundle, or sack (as appropriate) **MUST** be sent with a full unit address and contact telephone number written/stamped on back. If the unit is moving to a new address or being renamed, then the revised details should be included with the receipt.

18. MOD Form 24 must only be sent for items protectively marked as SECRET.

19. MOD Form 24 must be retained for 1 year after transaction or transfer has completed.

Forwarding Large Quantities of Records to MOD Archives

20. If you plan to send a large quantity of paper records to the MOD Main Archives, contact the DBS Knowledge and Information Services Contract Management Team advising the type and quantity of records involved. The Contract Management Team (CMT) will provide assistance with the planning and costing of the movement of registered files that are destined for the MOD Main Archives and will ensure that suitable provision can be made for their arrival. The CMT should be contacted for any queries on using the MOD Main Archives and they can be contacted by:

Email: DBSKI-RecordsCMTMgr@mod.uk

Telephone: (9)4240 5701 / 01869 259701

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

Retrieving Records from MOD Archives

22. If there is a need to consult records submitted to MOD Archives, originating units can request their temporary return by contacting the relevant MOD Archive. For records held at the MOD Main Archives an Asset Request Form should be forwarded to TNT Archive Services.

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

USING THE MOD SENSITIVE ARCHIVES

Background

1. **TOP SECRET** material or material requiring special handling **MUST NOT** be sent to the MOD Main Archives at Swadlincote. The following procedures **MUST** be complied with when depositing this material with the MOD Sensitive Archives at HMNB Portsmouth.

What you should do

2. Units should telephone or email 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)**).

3. Units must keep a record of **ALL** material sent to the MOD Sensitive Archives including the date of dispatch.

Registered Files

4. TOP SECRET files with a disposal recommendation of destroy **MUST NOT** be destroyed locally. As soon as they cease to be of business use, these files **MUST** be sent to the MOD Sensitive Archives where custody will be passed to the DBS Knowledge and Information Services Records and Review team.

5. Each registered 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 (the disposal recommendation) and destruction date – where applicable (Part 2 of the form); a branch stamp including full address/telephone number (at Part 3); and a signature of the reviewing officer of the correct grade (Band C2/Service equivalent or above).

6. File **titles**/numbers on covers are to be clearly legible.

7. Documents **MUST** be in Registered File covers – not Temporary Enclosure Jackets, branch folders, or **bundles** of loose papers, etc.

8. A copy of the MOD Form 262F **MUST** be retained by the unit as a record of all files archived at the MOD Sensitive Archives.

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

10. **Bundles** of files should be clearly labelled and strapped or tied together.

11. Empty **file** covers containing no other papers should not be sent to the MOD Sensitive Archives.

Unregistered Records

12. 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.

13. 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 security classification marking of the enclosed material, the year of its origin and the reason that its permanent preservation is being recommended must also be indicated. The DBS Knowledge and Information Services Records and Review team will keep one copy of the list and return the other as a receipt.

Receipts

14. A MOD Form 24 (Receipt) for each record, file, bundle, or sack (as appropriate) classified SECRET or above MUST be sent with a full unit address and contact telephone number written/stamped on back. If the **unit** is moving to a new address or being renamed, then the revised details should be included with the receipt.

15. MOD Form 24 must only be sent for items classified SECRET or above.

16. MOD Form 24 must be retained for 1 year after transaction or transfer has completed.

Retrieving Records from MOD Archives

17. If there is a need to consult records submitted to the MOD Archives, originating 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.

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

19. The MOD Sensitive Archives can be contacted at:

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

    Tel: 9380 25252

    Email: DBSKI-RecordsReview12@mod.uk

USING THE DEFENCE FILEPLAN

What is the Defence File Plan

6. A file plan is a structure for managing records in topic-based folders. The Defence File Plan combines a standard approach across Defence with the ability, using the Defence File Plan Taxonomy, for local design to reflect the work of each particular unit. It has been in use for several years.

7. We organise our information hierarchically by unit. Below the Unit reference (Electronic Unit Name), there will be a number of levels of **classes** and **folders**. Both classes and folders are containers of information. However:

- A **class** can only contain subordinate classes and folders (or folder parts) – it does not directly contain records;
- A **folder** can only contain records – it does not contain a mixture of other folders and records.

Structure of the Defence File Plan

The top level of class, Level 1, contains 4 **classes**:

- Class 01 – Administer the Unit
- Class 02 – Command or Direct or Manage the Unit
- Class 03 – Support the delivery of the Unit's Objectives
- Class 04 – Deliver the Unit's objectives.

Classes 01, 02 and 03

8. Each of Class 01, Class 02, and Class 03 has a set of other classes under it at Level 2. They don't all have to be there in your unit's file plan, but these are the only ones allowed at Level 2 for these classes. The set is as follows:

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

Level 1	Level 2
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 Operations

9. At Level 3 and below, the Unit can determine whether to have an additional level of classes, or folders which will contain the records themselves. The maximum number of levels is 6 … so if we get to level 6, that has to contain folders (or folder parts).

Class 04

10. The structure of Class 04 (Deliver) is at the discretion of the Unit, within the maximum of 6 levels. These classes should reflect a breakdown of the business unit's activities to deliver against its plan.

Naming Standards for Classes and Folders

11. As with file names, make the title meaningful and concise, and use the same allowed character set (see Guide Info 007). Only use abbreviations when they are well known and unambiguous.

File Plan Class Descriptions with Defence Taxonomy Terms and Generic Retention Schedules

12. The table below contains descriptions with Defence Taxonomy terms. It also contains generic retention schedules, indicating when the folder is to be reviewed (unless otherwise specified): these are shown as the number of years after the date of the last entry.

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	Administer the Unit		**The range of activities that enable the business unit's management to support its physical infrastructure and human resources.**			
01	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

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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	15 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	15 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	15 years

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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	15 Years (But with the intention of retaining some categories for 100 years.)

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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. • Unit's Liaisons • Unit's Affiliations • Unit's 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 15 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

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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	15 years

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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 wellbeing 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

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
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.**			
	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

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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	15 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

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
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'.**			
	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	7 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

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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	15 years

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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	15 years

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
	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.

Serial	Level 1 Class Name		Description	Potential Activities	Defence Taxonomy Classification	Generic Retention Schedule
		Level 2 Class Name				
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.**			
	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.

WHAT IS KNOWLEDGE MANAGEMENT?

1. Knowledge Management (KM) attempts to address the problem, for organisations, of tapping into the collective experience and expertise of its people. Such expertise is often intangible and unquantified. Some of it may have been recorded and stored on systems (possibly now obsolete), but much of it will be held simply in people's heads.

2. Good KM is difficult to achieve in practice, as it involves addressing elements of behavioural psychology, organisational culture, obsolescence management and storage & retrieval. It is worth attempting, however, even on a small scale, as the potential for business benefit is high.

Benefits of Knowledge Management

3. The benefits of good KM include:

- Expertise is shared and retained even when individuals leave an organisation.
- Expertise is easily identifiable.
- Teams have access to past experience and lessons learnt.
- Improved collaborative working.
- Improved networking.
- Knowledge "archived" for future (re-)use.
- Potential for innovation through making new connections and sharing experience and expertise.

Elements of Knowledge Management

4. The three main elements of KM are:

- **Knowledge sharing**: making knowledge available for others to use; and encouraging colleagues to share their own knowledge with others for mutual business benefit.
- **Knowledge capture**: techniques to extract, quantify, record and store the hidden expertise that employees have, over time, acquired, that improves their ability to discharge their roles competently.
- **Knowledge filtering**: possibly the trickiest element of KM: filtering captured knowledge to identify the elements worth retaining – that is, the knowledge that will be of continuing value to post holders and/or the organisation, as opposed to knowledge that is only of use to a particular individual.

Sharing knowledge

5. This is the single most important area of KM. Sharing knowledge and expertise allows people to make useful connections, share and try out new ideas, find (and offer) help,

6. Good methods of sharing knowledge include:

- Collaboration – face-to-face or through the use of technology-based tools (social media etc).
- "Who does what" directories.
- Networking (Communities of practice/interest, knowledge cafes etc).
- Case studies.
- Storytelling.
- Shadowing and mentoring programmes.
- Peer assists.

7. For knowledge sharing to work well:

- Make collaborative environments “safe” – treat each other with courtesy and respect.
- Encourage informality and a non-hierarchical approach where possible.
- Ensure the potential benefits are mutual and clear to everyone.
- Promote an atmosphere of trust and encourage leadership by example.
- Don’t do everything online – try to have some face-to-face events from time to time.
- Remove “barriers” – e.g. if someone is uncomfortable in a group environment, consider a one-to-one discussion.

Capturing knowledge

8. Techniques for capturing knowledge include:

- Handover notes.
- Inductions.
- Exit interviews.
- Lessons learnt exercises and After Action Reviews.
- Shadowing/Mentoring.
- Collaborative workspaces.

9. Things to consider when capturing and filtering knowledge are:

- Knowledge should be imparted freely – aim to persuade rather than coerce.
- Allocate enough time and resource, but don’t attempt blanket capture – aim for key points. You can only ever expect to capture a small proportion of the total knowledge and expertise held by individuals. Knowledge capture on its own will not be enough to address business KM issues.
- Consider the relevance of the “knowledge” being imparted. How useful is it likely to be? Consider failures as well as successes and always ask “why” in addition to “what” and “how”.
- Think about archiving and future proofing – captured knowledge needs to be retrievable, re-useable and refreshed.
- Ensure exit interviews are conducted and reviewed by individuals who understand the work area.

10. Finally, bear in mind that knowledge is not static: it is constantly changed, updated and refreshed as personnel come and go. Creating an environment where knowledge is “managed” effectively is not a quick fix. It takes time to change team or organisational cultures. If you implement a KM improvement programme, identify your main business priorities and risks, and tackle those first. Keep the momentum going, but do not try to change everything at once. Aim for incremental changes, allowing these time to bed in. Review, reflect and adjust as you go.

HOW TO DO A HANDOVER

Why do a handover?

1. Handover exercises, when moving from a post or stepping down from a project, help ease the transition for successors in the role. Well-conducted handover exercises benefit the business, and the individual. The business retains at least some of the knowledge and expertise acquired by the outgoing postholder. It also has assurance that the incoming postholder is starting out with a good basic knowledge of the workload and how it has been managed.

Tips for doing handovers

2. Make contact with your successor as soon as possible.
3. Schedule some discussion time. Ideally this should be face to face, but if it has to be done by phone, make sure you have both cleared enough time and ensure you will not be disturbed or distracted. The amount of time needed will depend on the amount and complexity of the work.
4. Talk through as much of the work as you reasonably can. If it is possible for both of you to look at work on screen simultaneously, do so. It is generally easier to understand something if you can look at it and walk through how to do it. If the post involves complex online activities, do at least one walkthrough together.
5. Ask questions as you demonstrate the work, to check their understanding. Allow them to do the same.
6. If you have time, write up a set of handover notes for the new post-holder to refer to. If time is short, ask them to write up an account of your discussion – which will check their understanding of what they have been told – which you can then quickly review for accuracy and amend as necessary.
7. Make sure they have details of any key contacts together with what those contacts do. Where possible, take them round and introduce them to people.
8. Make them aware of priority tasks and timescales or deadlines. Make clear what you have already completed and what remains for them to do.
9. Explain any routine or recurring tasks and any regular deadlines.
10. Try to make them aware of any particular processes, procedures, house styles, etc. that the business unit will expect them to use.
11. If time is really short, list the core aspects of the job that the new post-holder must know, and talk through them. Let them know if any relevant training is available and where and how to access it.
12. If possible, leave your contact details and let the post-holder know that you will be happy to offer advice, at least until they have found their feet.

EFFECTIVE INDUCTION

Why do inductions?

1. Inductions benefit both the new team member(s) and the team leader(s). Well-conducted inductions make sure the inductees:

- Know who their fellow team-members are and what they do;
- Understand the tasks associated with their role;
- Understand how their role fits into wider team objectives and ultimately Departmental outputs;
- Understand and know how to use office processes and procedures;

ensuring they feel comfortable and confident in their new roles. A good induction process will help new team members settle in quickly and minimise the number of times they have to ask for help or clarification.

Tips for conducting inductions

2. Make checklists (or do a spreadsheet) of everything you intend to cover so you can check off each element as it is done.

3. Have your own checklists and any information folders and/or desk manuals for the inductee ready in advance.

4. Make the inductee feel welcome. Introduce them to the team members and (ask them to) give a brief overview of what they each do. Don't go into too much detail on day one as it can be overwhelming. It might be worth getting the team together (as far as possible) for an introductory chat over coffee. A less formal setting may help people to relax and be more open.

5. Go through the everyday processes and procedures the new entrant will need to be aware of. These might include:

- Finance procedures. Who is the Business Manager? What financial authority (if any) does the postholder have? What authority do other team members have? What requires a business case and what doesn't? How is T&S authorised?
- Housekeeping. How are meeting-rooms booked? How are visitors booked in? Who keeps the Accident and Hospitality books? Is there an end-of-day checking routine for the last person to leave? How is stationery supplied? How does the teamsite function? Is the inductee familiar with the fileplan? With the Government Classification scheme? Do they know what, how and where to upload work-in-progress and where and how to file? Who does the team publishing to the Defence Intranet? What are the contact details for the relevant I-Hub?
- Training. Make sure the inductee knows which mandatory courses to complete and how to report completion. Are there any regular tasks such as answering PQs or FOIs and does the inductee need training in order to deal with them? Does the role have any particular tasking that will require immediate training?
- Business processes. Are there regular team tasks? Are they shared or are they allocated to specific individuals? What are the cover arrangements? How is leave organised and authorised? How often are team meetings held and are there standing agenda items? Does the inductee need to consult anyone (eg TLB focal points) on a regular basis? – if so, ensure they know who these are.

- Health & Safety. When are the fire alarms tested? Who is the Floor Liaison Officer? Where is the fire muster point? Who are the First Aiders and how should they be contacted? Who in the (wider) team is responsible for general H&S matters?

6. Once the inductee has been verbally briefed on the basic processes and procedures, ensure they have access to written reminders as far as possible. You might want to consider compiling a file or folder of leaflets and instructions, or have a folder on your teamsite specifically dedicated to induction material.

7. Talk the inductee through their new role. If at all possible, arrange a handover with the previous incumbent. Otherwise, try to have a desk manual available. If exit interviews relevant to the role have been compiled and stored, go through these with the inductee and ensure they have ready access to them for future reference.

8. If the role is completely new, talk the inductee through your understanding of, and expectations for, it and invite their views.

9. Remember: Don't overload the inductee on Day 1. If possible, try to stage the induction over a few days, to allow them time to absorb all the new information.

10. Make sure they know they can approach you for help while they are finding their feet. Make it clear it is fine to admit they don't know or understand something, and that it is better to ask than to struggle on blindly.

11. Arrange some networking and shadowing opportunities. For example, take them along to some meetings as an observer and introduce them to your contacts; get them to shadow individual team members; see if your Team Leader would be willing to have them shadow for a day etc. This will allow them to start building up a network of useful contacts for the role.

12. Avoid: A one-way-traffic situation. It's easy to work through checklists ticking off each piece of information you need to impart, but make sure the inductee has the chance to review his/her understanding from time to time. Try not to put them on the spot – sometimes it is a better idea to allow them time to process information by giving them a later opportunity to ask questions.

13. A new entrant brings with them a fresh perspective. As well as explaining to the inductee what you expect of them, ask what they expect of you, and what skills they can bring to the role and to the team. Induction is an excellent opportunity for all parties to exchange and share knowledge and expertise, and, done well, can be a good way of refreshing your own outlook on how you work.

MENTORING

Why mentor?

1. Mentoring someone can be useful professional development for both the mentee and the mentor. The mentee benefits from the experience and knowledge of the mentor. The mentor can gain a new perspective on the workplace by seeing it from the mentee's point of view. A good mentoring relationship should facilitate an exchange of knowledge on both sides.

Tips for successful mentoring

2. Meet with the prospective mentee face to face, ideally in an informal setting, before committing to becoming a mentor.

3. Discuss mutual expectations, agree aims and set boundaries in advance. For instance, consider (and agree):

- What the mentee hopes to gain from the relationship
- Whether this matches what you feel you are able to deliver
- How often you will make contact to review progress
- Where/how progress reviews will take place (e-mail, phone, face-to-face etc.)
- How and when the mentee can contact you outside of the scheduled catch-up sessions

4. **Note**: It is a good idea to schedule in occasional face to face chats if you can. Try to make these informal so that the mentee does not feel as if they are being interrogated. If meetings must be in an office environment, chat over coffee and not across a desk.

5. Once you have agreed a meeting/catch-up schedule, do your best to stick to it. Inevitably there may be times when you have to rearrange, but try to minimise these occasions, and ensure your mentee does the same. Unreliability can lead to mutual frustration and could potentially undermine the relationship. For the mentee, it may send a signal that you are not committed to the process, or them.

6. Agree how and in what circumstances the mentee can contact you outside of scheduled catch-up sessions.

7. **Remember**: A mentor is not a counsellor. Mentoring is about developing the mentee's professional capabilities. In any workplace it is inevitable that some personal issues will arise, particularly if the mentee has line management responsibilities. You may feel able to chat about such issues in general terms, but ensure you make clear from the start that you will not discuss named individuals or offer advice about specific cases as this could compromise your personal integrity. If you feel personal issues are endangering the mentoring relationship, call time and direct your mentee to professionals, such as HR or Welfare officers, who are more qualified to assist in these areas.

8. As a mentor, your role is to review, comment, suggest and guide, not dictate. As far as possible, if a mentee has encountered a problem or difficulty, try to help them arrive at their own solution – which may not be the solution you personally might choose. Try not to tell your mentee what to do; instead, encourage them to think through potential scenarios by asking open questions, eg:

- "If you do x, what do you think might happen?"
- "What are the advantages and disadvantages if you do y?"

9. If your mentoring is over a fixed period of time, have a final meeting to discuss the process with your mentee. Review the outcomes, discuss whether expectations were met, and establish what went well and what could have been improved. This will help both of you when mentoring opportunities next present themselves.

CREATE A DIRECTORY

Why create a directory?

1. Directories do not have to be enterprise-wide. Even in comparatively small teams, "who-does-what" directories can be helpful, particularly for team leaders and new entrants. Directories are also good starting points for finding subject matter experts within organisations – helpful if you are starting a project or dealing with an urgent task such as a PQ or briefing request.

Tips for creating directories

2. Make sure everyone understands the purpose of the directory in advance, particularly if people are expected to update their own entries. The directory will be much easier to maintain if people have bought in to the concept.

3. Decide on the format. You might want to use a collaborative workspace such as SharePoint (MOSS), Defence Connect or the Knowledge Hub, or a simple Excel spreadsheet. Whatever format you choose, make sure everyone knows how to access it and how to edit it.

4. Decide on the structure. Choose the fields you want people to complete. These might include:

- Name
- Contact details: room/floorplate/desk number; telephone; preferred email address
- Role
- Profession: eg KIM, Policy, IT, Legal, Commercial etc.
- Skills and qualifications
- Professional memberships

5. **Note**: Abide by Data Protection[13] principles where personal information about individuals is concerned.

6. Encourage people to expand on their role details, to explain what the role covers and what particular areas they are responsible for.

7. Skills can include specific skills, such as languages; recognised qualifications, such as MCIPS; or areas of particular proficiency, eg information assurance, procurement, copyright etc.

8. **Note**: Expanding on roles and skills in this way moves a directory from being a simple contacts list to becoming a source of expertise and knowledge.

9. Following the above will create a basic functional directory that should have lasting value to a team. However, depending on the functionality of the format you are using, you might want to consider some additions to the core structure:

- A facility to upload pictures of individuals
- An option to include a "personal statement", where people can introduce themselves in their own words. Have a template for this, and a word limit, so that statements are consistent in style and size, without suppressing individuality.
- A "Contact" or "Message" facility that is not email-dependent
- A "search" facility, particularly if the directory is likely to grow to a point where it will not be rapidly browseable. You may need to consider a metatagging facility for the directory fields.

[13] See the Data Protection landing page on the Defence Intranet : http://defenceintranet.diif.r.mil.uk/POLICY/INFO/DPA/Pages/DPAHome.aspx

10. **Remember**: Not everyone is comfortable with including personal information or photographs of themselves in open forums. Do encourage this type of contribution (and lead by example), but don't make it compulsory.

11. Once the initial directory has been created, schedule in update reminders. Updating directory entries is not likely to be seen by people as an urgent priority, and they are likely either to forget to update, or to continually defer the task unless they are prompted to do so. A quarterly or half-yearly "Please check and update your Directory entry" reminder, coupled with a "Please confirm", will help to ensure the directory remains current and functional.

NETWORKING

Why network?

1. Networks are good ways of building personal connections and expanding your range of contacts. Everyone has networks of some sort – family, friends, trusted colleagues – but it is not always easy to see the connection between this kind of personal networking and the wider professional networking that can help people work collaboratively, deliver projects or develop their careers. This guide aims to offer some ideas on how to set about building your professional networks in a constructive and productive way.

Tips for networking

2. Consider your personality type. Networking is often seen as synonymous with “working a room” – going round at a conference or business function chatting to people and making connections directly, face-to face. Certainly, if you are comfortable in this type of situation, this can be an excellent networking technique. However, for those who tend to be reserved, under-confident, or shy, face-to-face networking with strangers can be something of an ordeal. If you fall into this category, it is probably better to approach networking, initially at least, in a different way.

3. The best way to start networking is by joining in. The digital world offers many more opportunities to do this, and may also be a more comfortable environment for those who find face-to-face engagement difficult.

4. Start small. For face-to-face networking, volunteer to join a small work-related group where you already know (and trust) a couple of people. Alternatively, ask to shadow a colleague at a regular meeting they attend. In either situation, the people you already know can introduce you to the rest of the group, making those difficult first connections for you. Sit and listen to the group in action – this will give you a feel for the personalities involved. It will also let you find out what their key points of interest are. This will help you find topics of mutual interest to chat about with group members, and will help you start building on connections.

5. If you are comfortable with the technicalities of using social media, try looking for groups that focus on one or more of your particular interests. If you are not comfortable using public social media tools like LinkedIn or Twitter, see if your organisation, or your professional body, is using tools which are limited to their own communities, for example in Sharepoint or Defence Connect. Join a community of practice, or a community of interest (making sure it is regularly “active” – check to see that there have been recent contributions to it). Add a profile and photo if you want to, but don’t feel obliged to if you are uncomfortable with the idea. You do not need to start contributing immediately. It is a good idea to “lurk” for a while: watch what other people post to the group, read the comments on their posts and get a feel for how the community operates.

6. Once you feel you understand how the group works, and provided you feel comfortable with that, think about posting yourself. You might want to start by commenting on other people’s posts and build up to making your own contribution. If they comment back, or make a comment about one of your posts, you have made a connection – engage with the person and build on the professional relationship.

7. If you build personal networks in an online environment, you will almost certainly find this helps you network in the face-to-face arena. For example, if your online group organises an event – a training course, an evening meeting, a conference, a study day etc. – consider going along if you can. You will already have made the connections online, so you will almost certainly know some of the participants, and your online interaction will give you a conversational opening. They in turn can introduce you to other participants – and so your network continues to grow.

Useful sites for professional KM networking[14]:

8. Networking sites include:

Government

- **The Knowledge Hub:** Collaborative network for the public sector. Sign-up is free for people with a valid public-sector email address. Open groups are accessible to join and browse.

External

- **JISCmail:** Mailing-list-based discussion forums on a wide range of topics. Aimed at the Higher Education community, but free to join and sign up for Open Groups with browseable archives. Closed **groups** are also free to join but you have to apply to list owners for membership.
- **LinkedIn:** Has many sub-groups on particular topics, if you are comfortable with the public environment.
- **CILIP Groups and Regional Member Networks:** For **CILIP** members, but two groups come free with general membership – extra groups are £10 each.

[14] For all external social media activity, follow the policy and guidance on acceptable use.

ESTABLISHING COLLABORATIVE WORKSPACES

Why encourage collaborative workspaces?

1. Collaborative working can be a good way of sharing and benefiting from collective knowledge, experience and expertise. A shared workspace, group area or discussion forum can facilitate exchange of ideas, provide a single place to work on documents and tasks and generate discussion and comment. Good collaborative environments can be stimulating and informative. However, the theory does not always match the practice, and careful thought and preparation should go into set-up and administration.

Tips for collaborative workspaces

2. If you intend to use ICT to facilitate collaborative working, think about what you are trying to achieve and choose the most appropriate tool for the environment you want to create. These might include:

- MOSS teamsites
- Wikis
- Discussion forums
- Internal or external collaborative tools such as Defence Connect, the Knowledge Hub, Yammer, Huddle etc[15]

3. If possible, keep it very small scale to start with. Create team environments rather than organisational ones.

4. Consider the **90:9:1** principle. Paraphrased, this states that engagement levels in a collaborative environment will be 90% “lurkers” who never contribute; 9% “editors” who occasionally comment but rarely initiate discussion; and 1% “activists” who regularly post and comment, and whose voices therefore tend to dominate discussion. It is not a hard and fast rule, but it is something to keep in mind, especially when your collaborative environment is set up. If an “activist” group is evident, you need to try some techniques to encourage greater participation by the “editors” and “lurkers”. These might include:

- Setting up smaller, topic-specific, or team-based groups within your collaborative environment. People may feel more comfortable posting about a topic they know well, or to a familiar group of people.
- Ensuring new contributors are welcomed, and that their posts receive constructive comments, or even “liking” posts, if your environment has that functionality.
- Using “activists” to encourage and facilitate participation within their own teams

5. Make sure it is accessible to everyone in your target group. If that group includes participants external to your own team or organisation, don’t set up a workspace that only internal users can access. You may need to be prepared to make a business case for a commercial collaborative tool.

6. Make it a welcoming environment. Be as informal and egalitarian as possible and don’t hedge it round with too many rules.

7. Make it comfortable for people to use. Someone doubtful about the whole concept is unlikely to continue to participate if they receive negative feedback. Critical comment is often essential, but ensure comments are constructively expressed. Promote courtesy and moderate discussions.

[15] If you are using an external collaborative environment that has not been set up as a MOD-only workspace, ensure you follow the policy and guidance on acceptable use of social media

8. It should be obvious, but ensure the tools you are using work. Lack of speed, poor design, over-complexity will all turn potential users off. There is no point in posting a request for help if no one is alerted to that request. In general people won't search out material for themselves, so ensure there is an alerting mechanism that will notify them of new postings. Test functionality before going live.

9. Ensure everyone knows how to use it. Invest some time and resource in ensuring your team is properly trained, particularly if your collaborative environment is not particularly intuitive. Remember some people are very comfortable with experimenting and teaching themselves with the help of manuals, while others respond better to online or face-to-face training – try to have a mix of training available if resources allow.

10. If there are a large number of contributors and/or possible topics, consider some sort of filter mechanism – eg RSS feeds, creating special interest groups, etc. – that allows participants to be alerted to topics specifically of interest to them.

11. Encourage senior managers to lead by example, using the collaborative space for communication and comment.

Note: The presence of senior managers in a collaborative environment can encourage participation, but it may also intimidate the less confident. It is important to emphasise that engagement should always be constructive and any disagreement courteously expressed.

12. If possible, include a directory somewhere within your collaborative workspace. List the participants with contact details and add short profiles of what they do. Encourage participants to expand on those profiles, but be aware that not everyone is comfortable posting information about themselves – even in a professional context in a closed environment. Try to encourage, not coerce. Provide templates and a couple of example profiles to get things started.

13. Know when to discourage use of a collaborative environment. They are not suitable for everything, nor for everyone. Some people will never be comfortable contributing to a collaborative workspace. Unless you are going to remove all alternatives, thereby forcing use of the collaborative space, you need to allow for these people. Sometimes there is no substitute for a face-to-face meeting, with a team or with an individual, particularly if you want to be sure everyone has a chance to contribute ideas.

STORYTELLING

Why use stories?

1. Stories are not appropriate for every situation, but if, for example, you are trying to sell the benefits of something, a short, powerful illustrative story may well have more impact than a presentation based on statistics and projections. It is human nature to be gripped by a good story, well told. In the standard conference format, stories are particularly useful for "graveyard" slots, where you may need to work harder to hold your audience's attention. They are also useful for today's more informal type of events, such as "unconferences", where participants may be invited to do short 5-10 minute "lightning" spots on a topic of their choice.

Tips for good storytelling:

2. Match your story to your audience. Make sure it is an appropriate event for this type of presentation, and ensure it conveys the point you want to get across.

3. Base your story on the STAR format – Situation, Task, Action, Result.

4. Keep it short and punchy, simple and factual.

5. Good stories include an element of jeopardy: Outline the risk you faced. The audience is hooked by the need to know how the risk was averted.

6. Don't be melodramatic, and only use humour if you are reasonably confident of your comic timing. If you are not a natural storyteller, use a relaxed, anecdotal style. Practise as if you are telling it to your close friends – this will help you relax and make for a more natural delivery.

7. If possible, walk about. A story delivered in a static position from a lectern is likely to come over as rehearsed and stiff. Catch the eye of audience members from time to time as this will make you appear more at ease.

8. Props can be useful, but use them sparingly to illustrate, or reinforce a point. If you must use PowerPoint slides, keep them to a minimum and if possible use a portable mouse to change them, to enable you to continue to move around freely.

9. Avoid: Spin and jargon; "naming and shaming" individuals (or teams); and boasting. Try not to hector, patronise or lecture. All of these could antagonise your audience.

10. Not all stories need happy endings. Negative consequences can be just as powerful. You can tell a "We failed because…" story if it delivers a compelling message; or, if you can prove that the failure was down to the lack of the thing you are trying to sell to your audience – but be absolutely sure before you start that you can prove that.

11. Many good stories have a moral. Often, the lead character learns a valuable lesson. For stories told in a business context, the lessons that were learnt are an important element, regardless of whether the story has a good or bad outcome. Don't forget when telling a story to explain what you learnt from your experience.

12. If you really dislike the idea of telling a story yourself, but you think the technique might be effective, see if you can find a colleague or team member who would be willing to tell it for you. It's not unusual for two or even three people to share a platform, distributing the action according to their individual strengths.

13. Remember: The power of a good story is its memorability. It will stick in someone's mind long after a tedious presentation has faded away. If you want to share knowledge with a large group of people, and make it memorable, storytelling, provided your topic lends itself to the format, is a technique worth trying.

EXIT INTERVIEWING

Why do an exit interview?

1. When people change jobs or leave organisations, the expertise they have acquired over time in post often leaves with them. If they have been in post for a considerable length of time, this loss of this expertise and knowledge can be expensive. New postholders have to start from scratch. Useful contacts are lost. Processes, shortcuts, networks, ways to get things done – all have to be rediscovered or rebuilt. If a new postholder is taking over immediately, a handover exercise is a good way of attempting to capture and retain some of that knowledge. However, if a post is being gapped, or deleted, an exit interview gives the team leader a chance to try to discover what the leaver knows that isn't already set down somewhere, and bank it for future use.

Tips for conducting exit interviews

2. Make sure the environment is right. If the interviewee is not comfortable doing the interview in an open-plan area, arrange a private room. Make sure it has access to anything necessary to support the interviewee, eg a workstation where they can logon to their workspace to demonstrate as necessary, and/or internet access if they use the internet on a business basis.

3. If you need to understand their working environment – for example a laboratory, a library, an archive, a repair workshop etc. – schedule time to visit it and have them (allowing for any security issues) show you around and explain it.

4. Exit interviews with specialists should ideally be conducted by subject matter experts (SMEs) who can ask the right questions and assess the value of the output to the organisation. However, SMEs may dismiss some questions as being too obvious. It is useful therefore to have a non-specialist present who can ask these types of question to try to ensure the final interview record presents as complete a picture as possible. The local knowledge manager, if not themselves an SME, may also want to sit in on these interviews as they will give a good overall picture of the work of the business unit.

5. Ask the interviewee to list in advance what they think the key aspects of the job are. You might want to put a limiter on this – list, say, the five most important aspects of the job – or you might want to leave it up to them. Either way, their list will help you structure the subsequent discussion.

6. Be sympathetic to their state of mind. Someone leaving voluntarily is more likely to be co-operative and helpful than someone leaving against their will. In those circumstances, it can be helpful to stress that the leaver will be helping you personally, rather than the organisation – but recognise that sometimes you will have to accept that knowledge will leave with them.

7. Make sure they are comfortable with your chosen method of recording the interview. If you will be making notes, tell them at the start. If you want someone else to take notes for you, agree this with the interviewee in advance. Offer to let them review your notes, once written up, for factual accuracy.

8. Structure the discussion. Have a checklist of areas you want with appropriate questions relating to each area. You might want to consider:

- **WHO:** Who are the key people the outgoing postholder deals with?
- **WHAT:** What are the core tasks and key issues relating to the post?
- **HOW:** How does the outgoing postholder manage those issues and tasks?
- **WHEN:** Are there any particular tasks and/or issues that have deadlines attached? Are there any urgent deadlines?

- **WHY:** A very important question, particularly if you are looking to absorb the role into existing staffing structures. Effectively, what is the role's purpose? Why do its outputs exist? Why are they delivered in particular ways? What would happen if they were not delivered?

9. Don't stick to too rigid a structure – apart from anything else, that can easily seem too much like an interrogation, which can make interviewees defensive. Allow for an open conversational exchange, but gently steer the course back to your checklist if you feel it is veering too far off topic.

10. Good interview techniques apply to exit interviews as well. Listen properly. Check back to make sure you have understood. Ask open questions: "Can you describe…" "What helped you achieve…" "How would you set about doing…" etc. Guide the discussion and don't allow it to ramble.

11. To capture a discussion more fully, you might want to consider digitally recording it, either on audio or on film. If you have the means to do this, you must get the interviewee's agreement in advance. If they are uncomfortable with the idea of being recorded or filmed, don't coerce them into co-operating. If they can't be persuaded, revert to manual note-taking.

12. Ask them if they are willing to list their key contacts – but again be prepared for them to refuse.

13. Interviewees will have a lot of knowledge accumulated from years of experience. Some of it will be valuable to you; some of it will only be of value to them. For example, if they have developed a particular coping strategy for a task, ask yourself if it is good for coping with the task in general, or if it is good for helping them cope with the task. The two issues are different: the first may be of value to anyone faced with the task, whereas the second may only be of value to that particular individual.

14. Once the interview has concluded, compile an account of it and forward to the interviewee to check for completeness and accuracy.

15. Consider whether or not the completed interview is likely to have long term value. If the post is gapped only temporarily, the interview can be used to inform and support the new post-holder until they are settled into and comfortable with the role. It may not be required thereafter, as a further exit interview could be conducted when the post is next vacated. However, if the post is being gapped long-term, or permanently deleted, you will need to consider how best to archive the interview. This may be as simple as declaring it as a record and putting it on file, but if it has been digitally recorded, you may need to think harder about its long-term potential value and whether or not it will need to be flagged up as something that may require format-shifting to keep up with technological advances in future.

SHADOWING

Why Shadow?

1. Work shadowing can be an excellent way of transferring knowledge and sharing experience. However, for it to be properly effective, both shadows and hosts should observe some simple basic principles.

2. Once shadow and host have been matched, both need to give some thought as to the purpose of the exercise. A day or more where the shadow just trails around behind the host as they go about daily business will not be a rewarding or instructive experience.

Aims

3. The first thing to do is establish the main aim. This is usually either to learn how the host deals with specific tasks; or to observe the host as they deal with a typical day's /week's workload.

4. The first scenario might arise when the host is handing over to the shadow tasks that cannot easily be explained in written handover notes. Shadowing gives the host an opportunity to share more practical knowledge and go into more detail about their approach to tasks and the reasons why they are necessary. It also gives the shadow the chance to probe and ask pertinent questions.

5. The second scenario might form part of a general post induction/handover, or have been identified as a development activity for someone. In this case it is even more important to identify some secondary objectives in order to ensure the shadow genuinely benefits from the experience.

6. Once the shadowing has initially been agreed, shadow and host should have a discussion about how best to structure it. They should agree both the programme and the timetable, based on the shadow's expectations and the host's ability to meet them. The host should find out if the shadow has any particular areas of interest or concern, and try – as far as possible – to ensure these are covered in the programme.

Things to consider

7. It might be useful for shadow and host to consider the following points:

Shadow:

- Be prepared to take an active part in the exercise. Ask questions of your host and don't be afraid to say you don't understand something, or to offer an opinion.
- Review what you are being told and repeat back where necessary to check understanding. Ask your host if they would be prepared to review for accuracy any written notes you take during the exercise.
- Talk to any people to whom the host introduces you. If there is no time during the programme, but their work interests you, ask if they would be happy for you to get in touch directly. A shadowing exercise can be a good way of finding new and useful contacts.
- Tell the host if you feel you are being overwhelmed with information. If you are shadowing in order to learn particular tasks or processes, ask if the exercise can be done over a few days, so that you can assimilate what you have learnt and identify things you may need to go over again, or further questions you might have. If the shadowing must be done to a tight timescale, ask for a short break each time you feel in danger of being overwhelmed. Even 5-10 minutes of down-time can help you process what you have learnt and order your thoughts for the next stage.

Host:

- Are there any events in the programme where the shadow can actively participate? – eg meetings, team briefs etc?

- As far as possible, make everyone you will be dealing with during the shadowing exercise aware that the shadow will be coming along, and ensure they are comfortable with that.
- Are there any sensitive matters to deal with during the day? If so is there something useful and productive for the shadow to do while you deal with them? Or can they be shifted to a non-shadowing day?
- Ask the shadow for their thoughts and opinions where possible. Tell them in advance you intend to do this, and make sure they feel comfortable about contributing. If you intend to invite them to contribute in a meeting, make the other meeting participants aware in advance and ask them to make the shadow feel welcome.
- Review each part of the programme as it finishes and ask if the shadow has any more questions or if they would like to go over any part of it again. Try to build enough time in between events or tasks to allow for this.
- Try to strike a balance between adequate explanation of tasks or situations with which the shadow may be unfamiliar, and overloading them with information. It may seem obvious, but asking them what they already know will help you gauge how to pitch the information you give.

8. Finally, successful shadowing should benefit both parties. Obviously the shadow should profit from the host's experience and expertise. However, shadows also bring their own experience and expertise, and hosts should be open to their opinions and insights. A new pair of eyes may well bring a fresh perspective to daily tasks and routines. Good shadowing should leave both parties happy that they have gained from it.

RUNNING COMMUNITIES OF PRACTICE[4]

The widely accepted definition of Communities of Practice (CoP) is:

"Communities of Practice are groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly."[17]

Why use Communities of Practice?

1. CoPs have the potential to be as, or more, effective means of learning and sharing knowledge than conventional classroom-based or e-learning methods. However, they will not run themselves. In order for them to succeed, it is worth observing the following basic rules.

Tips for running Communities of Practice

2. **Focus on objectives**. Make clear the CoP's area of interest and do not allow the focus to drift. This may evolve over time but use each meeting (or on-line discussion) to ensure that activities are targeted at the needs of the participants. Do not be tempted to either dilute or broaden the scope of interest unless there is a specific change of circumstance which makes this necessary.

3. **Focus on learning.** A CoP differs from other informal or indeed more structured groups by focussing on the common theme of learning. Whilst CoPs can be used for problem solving, members do not ordinarily do project work together. However, the value of their learning within a CoP can often be realised through subsequent organisational project work.

4. **Good leadership is essential.** Voluntary, light-touch leadership is the essential element in making CoPs work well. Leaders need credibility, but may not necessarily be in a conventional organisational leadership role. Their style should be participatory and facilitative rather than hierarchical. Ideally two or three individuals should co-lead with each person taking responsibility for a different aspect of the CoP management (tasks can be rotated if necessary). This approach allows for optimum exploitation of different skills and provides continuity should a leader move on. Encourage CoP members to take a lead on different learning topics to help with their personal development and cultivate future group leaders.

4. **Define leadership roles.** Two of the most valuable when starting off a community are:

- **Agenda activist**: the person in this role maintains the focus on the CoP's stated purpose, and focuses learning activities on topics of specific interest.

- **Community keeper**: the person in this role enables effective relationships to develop and ensures that everyone's voice is heard, perhaps maintaining an informal chat group online.

6. **Be creative.** Keep the agenda alive by anticipating trends in the CoP's area of interest and use different exercises to add variety and appeal. Popular techniques include peer assisted discussions, Knowledge Café[18] style groups, expert presentations and interviews, and case clinics. Outputs should be captured as far as possible and posted to CoP workspaces. Doing outputs in FAQ-style format is one good way of making them readable and engaging.

7. **Establish and manage external sponsorship.** Identify a senior level sponsor for your CoP and keep them informed of progress. If they wish to make a more active contribution, you should welcome and encourage this. However, remind them that that their role is not to control or set the direction of the group but to inspire, participate and observe.

8. **Know how to access expertise and good practice .** CoP leaders do not necessarily have to be fully expert themselves. They should rely on the expertise of members of the group and bring in

[16] Adapted with permission from "Running communities of practice in practice" by John Carney, DSTL

[17] Jean Lave and Etienne Wenger, "Situated Learning: Legitimate Peripheral Participation", Cambridge University Press, 1991

[18] "A Knowledge Cafe is a means of bringing a group of people together to have an open, creative conversation on a topic of mutual interest to surface their collective knowledge, to share ideas and insights and to gain a deeper understanding of the subject and the issues involved." - ©David Gurteen

external expertise from time to time. Part of the purpose of a COP from a knowledge management perspective is ensuring that expertise is moved between those that have it and those that need it.

9. **Get the environment right.** A relaxed and attractive environment does a lot to create an atmosphere conducive to learning at the outset. Keep it fun and be sensitive to the different individuals' needs. Online environments should be accessible, easy to use and informal. In online situations, many more individuals will be anonymously observing activity rather than participating and this brings an additional challenge to managing the group.

10. **Recognise the time, effort and commitment involved.** Try to maintain regular face-to-face as well as online activity (meeting at least 3 times a year is considered good practice). Running a CoP takes time and effort – in some large organisations a Community Leader may devote a day a week in time, and more at the outset. If leading a CoP is expected as part of your job, ensure you are allowed enough time to devote to it. Recognise that you may have a personal commitment to your CoP members too – moving job means that you do not necessarily lose your obligations and involvement with a group, unless you are moving completely outside the CoP's sphere of interest.

11. **Focus on value.** This is particularly important where external stakeholders are involved, as there are inevitably cost implications. After each live event ask participants for feedback and follow up with an online survey or email questionnaire which should include questions associated with learning and application. Recognise that the value to participants is very different to external stakeholders. Think about the following aspects:

- Immediate value: the recognition of a useful meeting, a valuable and enjoyable experience.

- Potential value: what new relationships or insights have developed? Have people come back? How many documents have been downloaded? Has collective trust increased? Has best practice been shared?

- Applied value: typically realised outside the community itself – what have participants done differently as a result of their involvement (e.g. how many new people have they contacted)? Are there any good stories about applied learning? What is being done differently? Has performance or innovation improved?

- Realized value: to what extent can CoP activity be identified as contributing to the overall needs of the organisation, e.g. efficiency, effectiveness or profit?

12. **Take a long term view.** Reflect critically on your own development as a result of involvement as well as collectively with other members. Think about succession. Over time, well-run, fully-functioning CoPs can become influential entities within organisations and wider fields of interest.

DESIGNING AND USING ENTERPRISE IDENTIFIERS

1. Enterprise Identifiers refer to items of information which need to be individually referenced using a commonly implemented scheme. This allows common entities to be consistently named and defined across different systems, making it quicker and safer to integrate information from different data sources.

2. This guidance should be used by projects needing to uniquely identify entities within their systems.

3. When designing an Enterprise Identifier, you need to consider: Uniqueness; Scalability; Usability; Interoperability; Object Type; Backwards Compatibility and Future Proofing.

Uniqueness

4. All entities of a particular type must be uniquely identified. The system must not allow re-allocation of an identifier to mean something different from its original use. For example, Person Unique Identifiers must not be re-used for a different person.

Scalability

5. The system must be able to cope with the maximum foreseeable number of entries. The system must also be able to extend the number of different entity types supported.

Usability

6. The identifier system must be straightforward to implement and simple to use. Applications using it must be able to locate required entries quickly and easily.

Interoperability

7. The identifier system must be capable of supporting information exchange with likely partners (military, pan-Government, industry, etc). For military systems, this must include NATO.

Object Type

8. In order to identify the type of object concerned (eg unit, device, location, person), a unique Object Type Identifier must be used, capable of interpretation by all likely partners (including NATO for military systems). See JSP 604 for the issue and control of Object Type Identifiers.

Backwards Compatibility and Future Proofing

9. The identifiers should be compatible with existing systems, and be sufficiently clear and modular to interface with likely future projects.

USING AUTHORITATIVE REFERENCE DATA

1. Defence Information Systems should use the published set of Authoritative Reference Data. This will help Defence by:

- enabling interoperability between systems;
- reducing implementation costs for new systems;
- using consistent data;
- managing reference data more efficiently;
- establishing clarity over ownership and meaning of data;
- adopting common standards;
- improving management information.

2. There may be exceptions where use of the Authoritative Reference Data is not practical, such as systems which would be expensive to update or amend, or which have been designed to share information outside UK Defence, or where an integrated off-the-shelf system is being bought. However, in these cases the onus is on the project to justify why Authoritative Reference Data should not be used; the default should be to use it.

3. Authoritative Reference Data comprises Terms, Definitions, Lists of Values, and XML Schemas.

Terms

4. Terms are used to label content on Information Systems (such as the Defence Intranet, SharePoint and Meridio) to aid search, storage and retrieval. They are commonly referred to as subject categories and keywords and recorded as metadata in document properties. MOD publishes the UK Defence Terminology, comprising Taxonomy and Thesaurus, to contain these terms.

Definitions

5. Definitions are used in glossaries, and to provide clarity of meaning. They should be clear and brief and contain only that information which makes the concept unique. Additional text may be added in a note, but should not form part of the definition.

- Definitions may provide context for nouns such as “Tank” which have multiple meanings in the English language, where we need to be specific (eg that we are talking about a combat vehicle, rather than a liquid container).

- Definitions may contain information on Data Type, Length and Format (eg Data type of Character, and Length 20 for a Person Unique Identifier (PUID)).

Lists of Values

6. Lists of Values contain controlled values for a user to select, perhaps through drop-down lists. Examples include Military Ranks or International Country Codes.

XML Schemas

7. XML Schemas are used to provide standard methods of transferring information between systems. They allow developers to specify the structure of XML documents, with the data types and format of the information within the documents. Standard schemas (or fragments) are published in the Reference Data Manager.

DBS KI Responsibility

8. DBS KI is responsible for:

- maintaining high quality Authoritative Reference Data;
- publishing this through the Reference Data Manager and MOD Glossary (available on the Defence Intranet);

- maintaining the UK Defence Terminology (comprising Taxonomy and Thesaurus) to provide the terms for Subject Category and Subject Keyword metadata.

9. If you wish to propose content for update/inclusion in any of these services please contact DBS Management Information Centre of Excellence as per the details below or use the Contact Us option from within the MOD Glossary search homepage.

DBS Management Information Centre of Excellence (MICOE)
Tel Mil: 96161 4013
Tel Std: 01793 314013
Email: **DBSKIMICOE-DataSVCS@mod.uk**

USING ELECTRONIC UNIT NAMES AND ELECTRONIC ROLE NAMES

1. An Electronic Unit Name (EUN) is the abbreviated name for a unit that is determined by its Top Level Budget (TLB), or equivalent, and which provides a unique reference for electronic messaging and identification purposes. It is used to enable email addresses, or Electronic Role Names (ERNs) to be easily found, and to facilitate interoperability with other systems.

2. In this document:

- Unit refers to a unit as determined by the owning TLB, for inclusion in the MOD EUN List.
- Appointment refers to a post within a unit (also to accounts set up to support multiple users, typically group mailboxes).
- ERN refers to the entire name (i.e. Unit and Appointment). The general format for an ERN is: <**EUN** >-< **Appointment** >

Electronic Unit Name

3. TLBs are responsible for determining EUNs, and a central record of EUNs is held by MOD CDIO. Generally, EUNs must only be created to identify units that meet the criteria below and are not to be created for any other purpose.

4. When choosing EUNs, TLBs must aim for brevity, clarity and consistency:

- if the name is too long, it will be cumbersome and reduce the number of characters available to represent the Appointment;
- if the name is too short, it will lack meaning and be difficult to understand for those not familiar with the abbreviation.

5. The rules and guidance for establishing EUNs are as follows:

- In general, an EUN should be allocated at the level which corresponds to common understanding of what comprises a unit within that TLB:
  - In front line commands, a unit may for example be a ship or establishment, a Regimental HQ or Brigade, an Air Station or Squadron, while in the TLB HQ EUNs may need to be allocated at 2* or 1* level.
  - In Head Office the EUN is likely to be at DG or Director level, and in DE&S it may be a Project Team.
  - In independent HQs, EUNs should normally be the name of that HQ (however, no EUN can start with the characters of 'HQ' – a rule that is intended to promote clarity).
- EUNs should normally represent a real visible unit, in which MOD staff serve. There are a couple of exceptions used for administrative convenience:
  - Special group mailboxes advertised to the public (e.g. Low Flying);
  - To facilitate system trials.
- A unit is only allowed one active EUN at any one time. Therefore, when a new or replacement EUN is requested, the existing EUN must be deleted from the active column in the EUN database, and displayed in the legacy column against the new EUN. This will allow previous role names to be used during a limited transitional period, but prevent new ERNs being created using the old EUN.
- When requesting a new EUN, TLBs must identify the parent of the unit for which the EUN is requested. This is to enable organisational information to be constructed from the EUN list. The parent in this context is the unit which exercises immediate command authority. This principle applies regardless of whether or not the unit is hosted by a larger formation for administrative purposes.
- In general, Unit Names themselves should not be used to define hierarchy in command structure, unless it helps to differentiate between similarly named units.

- EUN is independent of location. Many units will have sub units located or hosted at different locations, but these can all share the same EUN.
- Consistency within TLBs is important. The same style of abbreviation should be used for all similar units.
- Bowman has specific data exchange restrictions. Therefore, where a Bowman Unit EUN exists, the identical name MUST be used.
- Where abbreviations are already in common parlance, then these should be used. However, where abbreviations are not currently used they should only be created when the gain from brevity will exceed any loss of clarity.
- The two basic syntax rules are:
  - An EUN can have a minimum one and maximum three parts, separated by spaces.
  - The EUN must be alphanumeric, with a maximum 16 characters including spaces - full details on syntax are in JSP 604 and the EUN Listings page on the Defence Intranet.

Appointment and Role Names

6. The Appointment must also optimise brevity and clarity. Names must follow common standards, both in the order, and through use of common abbreviations The rules and guidance for establishing the Appointment Names are as follows:

- The Appointment Title should reflect the organisational hierarchy within the unit (higher levels first), so that all appointments within a particular functional division are grouped together. Not every management level need be reflected, and it is better to avoid unnecessarily frequent change - title changes can incur costs and cause confusion.
- Hyphens can be used to separate different fields within the Appointment (up to a maximum of 4 fields). The first hyphen indicates where the EUN ends and the Appointment begins (see above). However, with the exception of ERNs that utilise Bowman systems, spaces are generally preferred; this is to aid readability within the Global Address List (GAL) and directories.
- Standard abbreviations for Appointments common to many units should be used whenever applicable. The list of standard abbreviations is published by DBS-KI through the Reference Data Manager (available via Defence Intranet) and can also be accessed through the EUN Listings page on the Defence Intranet; additions or amendments to this list should be submitted via TLBs to DBS-KI.
- Abbreviations specific to a particular unit may be used if no common abbreviation is available.
- Both upper and lower case may be used, and so can spaces.
- Where more than one short name is to be combined each element's initial letter should be capitalised within the compound, and spaces omitted (known as CamelCase). 'For example, Assault Pioneer Warrant Officer can be abbreviated to AssltPnrWO.
- The ampersand character (&) is not to be used.
- Use of specific rank, grade or title within Appointment Name is discouraged. However, if used it should appear at the end of Organisational Appointment detail.
- Appointments directly supporting senior officers should be given ERNs that will cause them to be sorted together with the Senior Officer Appointment.
- A role occupant's name must not appear in the ERN.
- Space and Round Bracket characters are stripped from the messaging address, while upper case and lower case are treated the same (so for example, 'ABC xyz' would be the same as 'abcXYZ'). Units must ensure that no duplications can occur.

- To enable automatic translation between the respective messaging systems, where there is a one-for-one match between a DII(F) appointment and a Bowman address, then the DII(F) appointment MUST be identical to the Bowman address.

- Appointments created for multi-access roles (e.g. group mailboxes or watchkeepers) will follow the same general rules as standard appointments. The appointment should be clear that it is for a multi access role.

- The full detail on allowable syntax is in JSP 604 and the EUN Listings page on the Defence Intranet. The two basic syntax rules are that:

  – Appointments MUST be alphanumeric, with hyphens or spaces as separators.

  – The maximum ERN length (i.e. EUN plus Appointment, and including hyphens and spaces) is 32 characters.

Registration Process for EUNs

7. Application forms for new or amended EUNs can be downloaded from the Defence Intranet. The process is also documented there, together with contact details of the parties involved.

8. The main areas of responsibility are:

- The TLB approves the application, checking that it conforms with the rules above;

- Where the EUN refers to a unit which may have BOWMAN, the application must be approved by the Land Environment Reference Information Capability (LERIC) on behalf of Signal Officer in Chief to assure compatibility;

- DBS-KI check the application to ensure compliance with CIO policy;

- The EUN database will be updated on behalf of CDIO (currently under the DII contract). The database will also be published on the Defence Intranet.

USING METADATA

1. Metadata is used to label information resources and is defined as data about data, or data that describes data. Content Management Systems, and Document and Record Management Systems, make extensive use of metadata, in order to add value to the user. In particular well managed metadata will:

- improve the speed and ease of finding relevant information by the attributes of documents or their content;
- enable search engines to be configured appropriately;
- support better content management by tracking owners, review and expiry dates.

2. MOD's metadata policy has been developed from, and meets the minimum requirements of, the current Government Metadata Standard. However:

- the currently published standard (e-GMS v3.1) is known to be outdated, and work is under way by the lead authority (The National Archives) to produce a new standard;
- users should apply the MOD Metadata Standard (MMS) to their data but, if there are better ways of achieving the desired result from the commercial software we are using, then the priority should be on providing the best user experience rather than slavish adherence to the standards.

3. Each case must be considered on its merits, and the implications of following standards different from those used by related systems must be taken into account. Where it is decided not to use the MMS, then the reasons should be clearly documented.

USING PERSON UNIQUE IDENTIFIERS (PUIDs)

1. The Person Unique Identifier is a unique universal key which MOD IT systems can use to identify an individual person who works in (or with) Defence, whether military, civil servant, or contractor. It is intended to provide a direct one-to-one link with that person, and is unchanged whether that person leaves employment with MOD, and later returns. For example, someone could be in the Royal Navy (and have an RN Service Number), then leave and join the Civil Service (and get a Staff Number); the PUID would however remain the same. The PUID is a 10-digit number (see below for detail).

2. Associated with the PUID is the PUID Name, which is a string of up to 20 characters, based on a person's surname (truncated if necessary) and initials, together with a 3 digit number to ensure that the PUID Name is unique to that person. The PUID Name can change (for example if a person changes surname), but it will remain tied to the same PUID.

3. All people working within MOD and who need to be recorded on our ICT systems must have a PUID. Other people may have a PUID if needed: examples include members of Allied forces working with MOD who need access to our ICT systems.

4. A PUID cannot be reused for another person.

5. An individual should not have more than one PUID.

6. The PUID is based on a 32 bit size and the numbering will start at 1,000,000,000. It will therefore always have a 10 digit length.

7. The method of registration for PUIDs is controlled by MOD CDIO. It is currently executed through the DII contract.

8. All new MOD applications using personnel data should have the ability to use the PUID scheme.

USING UNIT IDENTITY NUMBERS (UINs)

1. A Unit Identity Number (UIN) is used to enable Information Technology systems to identify units, sub-units, organisations or groupings of organisations within MOD, and to link the unit to a location. The major uses of UINs are:

- Asset Management
- Liability Management
- Financial Management
- Liability Planning
- Location Information

2. There are two types of UINS, described further below:

- Standard UINs
- Non-standard UINs

3. UINs are fundamental to the MOD's finance systems, and allocation of UINs must therefore take account of the structure of the Departmental Chart of Accounts.

4. UINs are maintained through use of MOD Form F942. This form should be used for all aspects of UIN maintenance including creation, title/address changes, and End Dating – changes must be notified promptly. Detailed guidance on completion of the form is published on the F942 Intranet Page; this guidance includes the routing and authorisation procedures, and how to check whether there is an existing UIN.

5. The responsibilities for UINs are:

- Overall policy - Chief Digital Information Officer (CDIO)
- Submission of requests for UIN changes – Unit (or TLB)
- Authorisation of UINs within their Command - TLBs
- Husbandry of Standard UINs - Army Information Services (AIS) Branch, CBM Division, Army HQ.
- Final authorisation of all non-standard UINs - Defence Equipment and Supply Chain Management (DE&S SCM).
- Husbandry of non-standard UINs - Defence Equipment and Support, Joint Support Chain Services (DE&S JSC Services).

6. With the exception of Custodial Accounts (CA UINs) where units are holding stock to be issued to others, no unit or sub-unit is to be allocated more than one UIN.

Standard UIN

7. The Standard UIN database is held on SIMS. It can be searched from DII via this link.

8. A Standard UIN comprises 6 characters in the format A9999A:

- Character 1 - alphabetic representing the Command as in the table below:

Character	Command
A	MOD (A) / Army
B	Infrastructure Accounting Army
D	MOD Central / Joint Forces
F	MOD (RAF) / RAF

J	Non Budgetary UIN
N	MOD (Navy) / Navy
P	Defence Equipment & Support
T	Army / Combined Cadet Force

- Characters 2-5 – four numeric characters which, together with the preceding and following alphabetic characters, will make the UIN unique.
- Character 6 – alphabetic, where A represents a unit, and any other character represents a sub-unit (note – letters I and O are not to be used).

9. Although Special Forces units and any UINs associated with them must be authorised by JFC, the first character in their UINs will reflect their Command.

10. When a Standard UIN is no longer required, then it should be given an End Date, after which it may no longer be used for financial or supply transactions. However, it should be noted that a UIN cannot be End Dated if there are sub-units that remain extant.

11. Army Units deploying on Operations will normally use a separate Operational UIN, instead of their own peacetime UIN. Applications are to be made on F942 before deployment in accordance with Army HQ instructions. An Operational Unit Title will be allocated to all Operational UINs and this name will generally remain for the duration of the Operation. On roulement Units will take over this title in Theatre.

Non-Standard UINs

12. Non-standard UINs are entered on the Stores System 3 (SS3) which is maintained by JSC Services. Non-Standard UINs are used in supply chain management, and further details can be found in JSP 886 (Defence Logistics Support Chain Manual), in particular Volume 3.

13. Non-standard UINs are in the format of a 2 alphabetic character prefix, 3 numeric characters followed by an alphabetic character (note – letters I and O are not to be used). The allowable prefixes of Non-Standard UINs are:

Prefix	Use	Users
CA	To manage stock on behalf of the Joint Support Chain (JCS).	Joint Support Chain Services (JSC Services) Royal Engineers (RE) and Royal Logistic Corps (RLC) contractors when authorised.
CB/CC[19]	To allow Delivery and Project Teams to authorise contractors to receipt and consume stock in support of contracts.	Defence Equipment & Support (DE&S) Delivery and Project Teams
CP	To manage the issue of materiel to contractors for contract repair.	DE&S
CQ	To enable issue of stock to contractors for disposal.	Defence Sales Agency (DSA)

[19] When all available numbers have been issued, this series can be expanded to include the additional prefixes of "CD", "CE" etc.

Prefix	Use	Users
CR	To manage repayment issues to other government departments and contractors.	JSC Services
CW	To manage the issue of operational stocks held as war reserve.	JSC Services
NP	To manage the issue of materiel to sea cadets/scouts and combined cadet forces.	Navy Command