JSP 441
Managing Information in Defence

Part 1: Directive
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 (e.g., 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

Defence Information Policy ................................................................. 1
Our Responsibilities ................................................................. 3
Rules for Managing Data ........................................................... 8
Rules for Managing Records ......................................................... 11
# 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.

Governance

- 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:
  o action on the subject covered by the folder has come to an end;
  o nothing has been added to the folder for the last year;
  o the folder contains 100 enclosures;
  o the folder has been open for 5 years;
  o annually on 31 December (electronic folders);
  o 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.