DEFENCE INFORMATION MANAGEMENT POLICY

This policy is issued by the Chief Information Officer.

The Sponsor is:

Head of Information Strategy and Policy
Chief Information Officer
Ministry of Defence
Main Building
Whitehall
London
SW1A 2HB

TABLE OF CONTENTS

INTRODUCTION

1. This is the **Information Management (IM) Policy for Defence**, issued by the Chief Information Officer (CIO), and applicable across Defence. It tries to demystify IM and help improve our collective ability to manage and exploit information more effectively. It contains:

- an overview of why Information Management matters;
- a set of policy groupings, each comprising;
  - context, providing a narrative of the background and objectives;
  - supporting policy statements, beginning "The MOD will"; these define what will be done (and in most cases already is being done) either directly by CIO, or by Top Level Budget (TLB) holders or other organisations on behalf of CIO);
  - performance monitoring, also beginning "The MOD will"; this defines what will be done by CIO or TLBs to assess effectiveness of the policy;
- an introduction to the Information Management Protocols, Handbook and Maturity Model;
- references to other key Information Management documents.

WHAT'S THE SCOPE

2. The scope of this Information Management policy is **information in recorded form**; this will therefore include many types of document (for example letters, publications, websites, spreadsheets, and databases), and many types of recording media (for example paper, electronic files, video tapes).

3. The policy applies across Defence. It aims to be realistic in recognising the exceptional conditions of front line operations, where neither the IM tools nor the time are likely to be available to people, and priorities are very different from office environments. Nevertheless, all the same principles apply.

4. Knowledge which is held in people's heads, and information which is communicated orally, are both out of scope of this policy, even though many of the general principles still apply. However, as soon as such information is recorded, then it becomes in scope.

5. The infrastructure on which information is stored and communicated, and within which data may be backed up and recovered, is also out of scope of this policy. The processing power of modern computers and the capacity of networks have made it possible to provide instantaneous communication and information access, irrespective of physical location. The MOD is seeking to provide an information infrastructure to link all of its Units, providing appropriate access to all staff; where practical, it will enable MOD information to be available to any authorised user, within appropriate security and access constraints. This policy document therefore refers to the infrastructure, which is of course a key enabler of effective Information Management, but does not define the MOD's requirements of it.

WHY DOES THIS MATTER?

6. The MOD needs to get more value out of information so that the Department can be as effective as possible. This **Information Exploitation** (IX) applies equally to all aspects of our work, from the office to the front-line, and is defined as:

> `*The sharing and use of information to support situation awareness, planning and decision-making and the coordination of desired effects.'*

7. In other words, IX is "*Getting good value out of the information we have*". To be good at IX, we first need to manage our information well. The aim is to make our information as good, as secure, and as accessible as it realistically can be. This IM Policy document, together with the IM Protocols, the IM Handbook, the IM Maturity Model and the other publications referenced here, are designed to help us do just that.

8. The MOD definition of **Information Management** is:

> `*A set of integrated management processes and services that enable and support the capability of collectors, producers and users to store, locate, retrieve and transform information, allowing it to become the right information in the right form and of adequate quality to satisfy the demands of the commander or organisation.'*

9. A shorter, informal definition of IM would be "*Recording and handling information so that we can readily find and use it again*". Good IM encompasses all of those things we do with information – like capturing, organising, communicating and retrieving it. Although we may never be able to manage information perfectly, the better we do it, the more effective we will be.

WHAT DO WE WANT FROM INFORMATION?

10. We want **information to be of good quality**. At best, we want it to be accurate, unambiguous, concise, clear, consistent and timely. We also like to know its origins (**provenance**) and **status** (such as historic or current, draft or final) and we want it in a form we can **access and use**. We also want to be able to **find and retrieve** it easily and quickly, confident that it remains **protected** from those people who shouldn't be able to see it. **Accessibility, security and privacy** are competing themes, so skills and sound judgement are needed to strike the appropriate balance between them.

WHAT DO WE NEED IN ORDER TO MANAGE OUR INFORMATION EFFECTIVELY?

11. If we manage some key generic elements of Defence information successfully, we will have solid foundations for improved information exploitation:

- **PROCESSES** – ensuring that key information activities are embedded into our normal routine - how we organise, store, secure, protect, share, label, and communicate information, for example;
- **ORGANISATION** – establishing structure, lines of communication, roles and responsibilities, authority, delegation;
- **CULTURE** – building the right culture to value, communicate, protect and preserve information, together with developing individual and team skills;

- **INFRASTRUCTURE** – deploying, supporting and maintaining the appropriate hardware, software and networks for capturing, storing, communicating and retrieving information.

OTHER THINGS WE NEED

12. Successful information management takes time, effort, care and discipline. It demands good, capable people – a few highly motivated and capable specialists ready to take the lead, identify good practice, develop viable ways of working and help others, together with a workforce that understands why management of information is important, and is able to put good IM into practice. Leadership is critical; if the command at unit level is committed to effective IM, then success will probably follow.

13. Although IM is an essential part of everyday business, there are always going to be other demands on people's time, and sometimes other constraints will get in the way. Although this policy sets out the intent, we recognise that it won't always be possible to meet it in full.

POLICY GROUPINGS

14. This document sets the context and defines the MOD policy for processes, organisation and culture as they relate to information, referring to infrastructure as appropriate. The overall aim is to manage, and hence exploit, our information better. All aspects of IM are inter-related, and there are no clear dividing lines between them. It is, though, helpful to group the context and policies together in categories, and here are the seven headings chosen. The first five refer to the processes, the last two to organisation and culture respectively.

a Management of Information as a Corporate Resource throughout its Lifecycle;

b Organisation of Information;

c Accessibility, Security and Privacy of Information;

d Information Quality Assurance;

e Communication of Information;

f Information Management Governance;

g Culture, Skills, and Personal Responsibility.

15. Note that these groupings are not the same as the eight IM components as used in the IM Handbook; this reflects the different scope and objectives of the two documents, rather than any difference in the overall message.

FEEDBACK

16. Comments on this document, and proposed amendments, should be addressed to:

CIO-JSP747-Enquiries

POLICY GROUP 1

MANAGEMENT OF INFORMATION AS A CORPORATE RESOURCE THROUGH ITS LIFECYCLE

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

18. There are many good reasons for recording information carefully:

- having the right information at the right time is critical to good decision making;
- good records avoid unnecessary duplication of work;
- reliable records form a sound basis for future work, analysis, audit, or historical record;
- records enable the MOD and individuals to justify or explain actions;
- records that are correctly stored (and so are readily found) assist the MOD in complying with information law, in particular with the Public Records Act, the Data Protection Act, the Freedom of Information Act, and the Environmental Information Regulations.

19. **A record is any recorded information of significance**. A record may, for example, be an action, a policy, a decision, a report, a plan, or a proposal. Deciding what is significant requires judgement, but if the information has any corporate or historic value, then it must be treated as a record. Three general principles apply:

- if the subject matter is of major importance (including, but by no means limited to, departmental strategy, operational activities, or major financial commitments) all related documents should be retained as records;
- for more routine subject matter, final documents should be retained, but not necessarily drafts, emails or other transitory material;
- if in doubt, keep it.

20. Some MOD systems distinguish between documents and records, where the main difference is that documents can be amended or deleted, but records can not be altered. This is however not a formal definition; legally, any document owned by the MOD is a public record. The important issue here is that, when using systems that distinguish between documents and records, people understand what sort of documents should be declared as records, know how to declare them, and actually do it. This Information Management policy does not make any such distinction between documents and records; as stated earlier, it is about information in recorded form.

21. A record could be in electronic form, such as a word processor document, an email, a spreadsheet, a web page, a digital image, an audio or video file; it could also be in hard copy, such as a signed contract, a printed photograph, a booklet, or a handwritten sheet of paper.

22. Inevitably the MOD prefers **records to be of good quality**; the value is higher if the information is written clearly, with the context, date and time, stating who was involved, and who took the record. However, it is better to have records of lower quality than none at all, as long as we are not misled into believing they are more authentic than they really are.

23. There are some **activities which must have a written record**, in particular key business decisions affecting allocation of significant staff time or public money, together with the evidence on which such decisions were made. In the front line, a **comprehensive and accurate operational record is vital**, notwithstanding the difficulties of producing it. Written records should be accompanied where appropriate by graphic, audio or video records.

24. **Records must be stored in appropriate shared areas** (electronic or paper), **and protected** by the appropriate security and access permissions. If off-line storage (such as local DVD/CDs) has to be used for record-keeping, then it must be formally controlled by IM staff; at the first reasonable opportunity the records are to be transferred into appropriate shared areas. Where the unit lacks access to such shared areas, then information must be passed periodically to the TLB or other unit for storage.

25. In order to promote the use of shared areas, electronic file storage allocated to individual users for personal use will be strictly limited; these personal areas of file store (including mailboxes) should be used only for material that is transitory (e.g. initial drafts, minor correspondence), or genuinely personal to the individual. Significant business-related material must be moved into shared areas. Storage described as Personal is subject to monitoring, both to ensure compliance with the MOD Acceptable Use Policy, as well as to deter incorrect storage of significant corporate information.

26. All information goes through a lifecycle, from the time it is originally captured, created or recorded, through to the time of its disposal. Some information recorded on MOD systems is of value only for a very short time; other information, and it can be hard to predict which, will be of value for decades, even centuries. It is therefore essential that all information that comes into the MOD domain is properly recorded in the right location. It must be carefully managed through its lifecycle, which may take it through a variety of different storage environments under the control of different owners; at all times there must be clear responsibility for its management.

27. **Each area of storage on MOD systems must be the responsibility of a Unit** and its command, in particular the Senior Information Officer[1]. This responsibility is exercised through the iHub[2] (or any alternative structure agreed by the TLB) and includes the setting of the appropriate access permissions to ensure that material is both adequately protected and sufficiently accessible. The information remains the responsibility of the Unit until either the Unit is disbanded, or the information is transferred to CIO Corporate Memory.

28. All information in shared storage is to be in a container (typically an electronic class, folder or file, or a paper file) **with a defined retention period**, determined in accordance with the Defence Records Management Manual (JSP 441).

[1] see Policy Group 6 – Information Management Governance
[2] Information Hub, or iHub - see Policy Group 6

29. Information within such a container is normally not to be weeded, except where it is a draft superseded by subsequent drafts or final documents. Even then, drafts on particularly contentious issues should be retained. Duplicates (arising perhaps from the same document stored with different file names) may be weeded.

30. Information in structured data stores, such as spreadsheets and transactional databases is, by its nature, volatile and subject to frequent update. Though it is impractical to retain snapshots of each change, it is important that the key outputs, or the contents of the data store at certain times, are treated as other documents, and retained for an appropriate period; the general principle of managing information as a corporate resource through its lifecycle applies.

31. JSP 441 contains the instructions for disposal of containers (folders). In general, these can only be destroyed locally if they are of no further value, and relate only to the administration of the Unit concerned. Otherwise the container is to be transferred to CIO Corporate Memory, within the timescales defined in JSP 441.

32. When a Unit is disbanded, ownership of all its information must be transferred, either to a successor Unit, or to CIO Corporate Memory.

33. CIO Corporate Memory, in conjunction with The National Archives, is responsible for determining which records are worthy of permanent preservation (transferring them to The National Archives), which records need to be kept by the MOD, and which should be destroyed, in accordance with the Public Records Act.

34. Not all information is in documentary form; the same principles of managing information actively through its lifecycle apply to other information stores, such as transactional databases. Such systems must be designed and configured so that their key outputs can be captured, retained, and capable of presentation in a format that is intelligible to a human reader.

Supporting Policy Statements - Policy Group 1

Management of Information as a Corporate Resource through its Lifecycle

35. The MOD will**:**

a. require information of significance to be recorded in shared areas on its systems;

b. require all information to be controlled at Unit level through iHubs;

c. require Units to control access to shared areas by setting appropriate privileges at class or folder level;

d. establish a reliable and sustainable mechanism for managing information through its lifecycle;

e. maintain an organisation (CIO Corporate Memory) responsible for acceptance of all shared information no longer required at Unit level;

f. publish detailed instructions on managing electronic and hard copy records (JSP 441);

g. transfer information worthy of permanent preservation to The National Archives.

Performance Monitoring - Policy Group 1

Management of Information as a Corporate Resource through its Lifecycle

36. The MOD will:

- collect, analyse and publish data on where information is being stored;
- monitor material held in personal storage areas;
- require Units to review their information storage on a regular basis;
- check that appropriate business and operational records are being collated.

POLICY GROUP 2

ORGANISING INFORMATION

37. Within the MOD, information flows quickly and accumulates rapidly. If the right information is to be available in the right place at the right time, then it must be easily retrievable from shared storage areas. Although different systems use different processes and technology, the principle of organising information logically applies to them all. Various methods of organising information can be used, depending on the nature of the information being handled, the capabilities of the system for storing and retrieving information, and the requirements of users of the system. Typically these methods will involve:

- hierarchical or numbered file plans (which may be in electronic record management systems, on NTFS (or other) shared drives, or on paper);
- content management systems within structured intranets;
- document libraries within collaborative working areas (team sites);
- labelling of folders, documents and records, using standard conventions;
- indexing by content or by date;
- attaching metadata (data about data) to folders, documents and records, containing subject classification from the Defence Taxonomy, key words, originating Unit, author, date etc;
- labelling of tables, records and fields within databases, and defining the appropriate relationships;
- labelling worksheets, rows and columns within spreadsheets.

Supporting Policy Statements - Policy Group 2

Organising Information

38. The MOD will**:**

a. define how information is to be organised in any major corporate system;

b. define standards for labelling documents;

c. maintain and publish a Defence Taxonomy, Thesaurus and Metadata Standard;

d. provide clear documentation with each system, supported by training where necessary, to explain why and how information is to be organised.

Performance Monitoring - Policy Group 2

Organising Information

39. The MOD will**:**

- review organisational file plans;
- conduct periodic reviews of Unit documents, records and structured data stores, to assess compliance with standards;
- undertake quality assurance of user guides provided with its systems.

POLICY GROUP 3

ACCESSIBILITY, SECURITY AND PRIVACY OF INFORMATION

40. The MOD must manage its information to ensure appropriate levels of accessibility, security and privacy. Accessibility (in this context) is about letting the right people have information, while security and privacy are about ensuring that the information is withheld from those who should not have it.

41. All staff are required to **share information responsibly and sensibly**, and information that has been recorded on MOD systems should, in general, be available to those people within the department who have a legitimate interest. However, this does not necessarily mean universal access. Information that is (or should be) protectively marked should be limited to those who genuinely need access to it. Sensitive information on individuals must also be marked, and access strictly limited to those who need it to perform their duty.

42. Access should be controlled by the use of protective markings, descriptors, national caveats, and code words, observing the definitions in the Defence Manual of Security (JSP 440), and through access privileges (typically based on user account in electronic systems). Where a decision has been taken to limit access, the **information must be protected and labelled** properly. It must also be stored in an appropriately secure storage location; documents must not be held in a place (electronic or paper) which is not cleared for their level of protective marking. Irrespective of how the document may be labelled, it is normally permissions set at the storage location that permit or deny access, and particular caution is required when changing permissions of existing folders.

43. Initial responsibility for determining the required accessibility and security of a piece of information lies with the originator of the information (i.e. the person who first creates the information, or captures it on behalf of the MOD), seeking advice as necessary. It then becomes the responsibility of the owning Unit, and in particular its Information Manager and Information Support Officer. However, everyone needs to be alert to whether a particular piece of information has been made sufficiently accessible or secure, advising the owning Unit as necessary.

44. **The Defence Intranet should be used for published information that is of potential interest across the MOD**, and should contain the authoritative version of such information. However, the Defence Intranet is not a record repository; the formal record must be held within the owning Unit's shared storage. This formal record should contain, as well as the information published, the date of publication to (and removal from) the intranet, together with the rationale for significant changes in published material.

45. Some specific systems support publishing, with or without access restrictions, and these should be used to contain (or link to) information likely to be of local interest, such as the work of a particular team. The technology should support wide and timely access to published information in these environments, and MOD staff need the skills to exploit it.

46. Information is often shared between the MOD and other parties, such as other government departments, allied or partner nations and forces, and commercial suppliers; this demands particular caution to avoid inappropriate release of material (whether through reasons of security, privacy or copyright).

47. There are two other meanings of the word accessibility in common use. Accessibility is the term used to denote how readily people with disabilities can

access electronic information, particularly on web sites. The MOD will comply with law and Cabinet Office guidelines on all internal as well as external sites (recognising that in certain operational systems, other priorities will take precedence).

48. The word accessibility is also used to define the ability to access information services successfully. Deployed units are often unable to access sources of information because of little or no connectivity to the place where that information is hosted, while even fixed units must allow for the occasional loss of access. This has implications for all. Deployable units must have local copies of important information, routinely updated when accessibility permits. Those supplying information critical to deployed units must allow for limitations of connectivity. Fixed units must include in Business Continuity plans how they intend to access critical information if normal channels are unavailable.

49. The MOD is subject to a wide range of legislation on information access and privacy, in particular the Data Protection Act, the Freedom of Information Act, and the Environmental Information Regulations, and is committed to complying.

50. The MOD's official internet presence (sites currently in the mod.uk domain, together with those others scheduled to move to that domain) is to promulgate its news and information to the outside world; to provide information to jobseekers, veterans and former employees, suppliers and customers; and to publish material released under the Freedom of Information Act. It is not, in general, a formal channel of internal communication, except in circumstances where other channels may not be appropriate, such as Business Continuity.

Supporting Policy Statements - Policy Group 3

Accessibility, Security and Privacy of Information

51. The MOD will**:**

a. maintain and publish clear and concise information security and access policies (JSP 440, JSP 400);

b. maintain and publish a list of protective markings, descriptors, national caveats, and code words (JSP 440);

c. provide appropriate information infrastructures, capable of supporting security and access requirements;

d. require Units to establish appropriate access permissions on information storage;

e. require staff to label information with the appropriate protective markings and descriptors;

f. provide documentation and training in information security, privacy and access;

g. maintain the Defence Intranet, for publication of material of interest across the department;

h. maintain a domain on the Internet, publishing appropriate material into the public domain.

Performance Monitoring - Policy Group 3

Accessibility, Security and Privacy of Information

52. The MOD will**:**

- require SIOs and Unit Security Officers to undertake periodic reviews of accessibility, security and privacy of information held within each Unit;
- investigate shortfalls of accessibility, or breaches in security or privacy, to reduce risk of repetition;
- monitor compliance with information access requests;
- independently review its external and internal web sites for content, quality, accuracy, and compliance with accessibility standards.

POLICY GROUP 4

INFORMATION QUALITY ASSURANCE

53. Decisions should be based on the best quality of information available to the decision-maker at the time. Information must be of **sufficient quality, in content, accuracy, relevance and completeness**, for the intended purpose. Perfection is rarely achievable or necessary, and there is often a trade-off between time, cost and quality; focus should be on delivery of the best balance between these three for the recipients of the information. It is critical in decision-making to know the quality of the information on which the decision is being made.

54. Training and education, supported by experience, are important factors in assuring information quality, and so are rigorous processes; published national or international standards, such as BSI BIP 0008 (Legal Admissibility and Evidential Weight) and ISO 9000 (Quality Management) appropriately applied, can be of value, and may be mandated for use within particular systems.

55. Information Assurance is another key aspect of quality. It is what we do to protect and defend information and information systems by ensuring their:

- Availability (reducing risk of loss of service);
- Integrity (avoiding unauthorised modification);
- Confidentiality (avoiding unauthorised disclosure);
- Authentication (validating the source of information);
- Non-repudiation (confirming that information has been sent and received).

56. Higher levels of information assurance normally attract a price, so the trade-off between time, cost and quality remains.

Supporting Policy Statements - Policy Group 4

Information Quality Assurance

57. The MOD will**:**

a. train staff to create or acquire high-quality information quickly;

b. train staff to assess the quality of information, and qualify it where appropriate;

c. establish procedures that embed the required level of quality in any information-handling activity, conforming to national or international standards where appropriate;

d. provide a feedback loop for comments on published material.

Performance Monitoring - Policy Group 4

Information Quality Assurance

58. The MOD will**:**

- continually assess systems for information assurance, identifying shortfalls in required levels of availability, integrity, authentication, confidentiality and non-repudiation;
- monitor the effectiveness of systems in delivering the right information on time, from the perspective of units, especially those in operational theatres;
- undertake routine surveys, seeking comments on the quality of information received, and canvassing suggestions for improvement.

POLICY GROUP 5

COMMUNICATION OF INFORMATION

59. Information is most valuable when it is available to the **right person at the right time, in the right format, and to the right level of quality**. All information-related activities must be targeted to this end. Information overload can be as detrimental to effectiveness as lack of information. It is therefore important to use the available tools wisely, prioritising communication, and organising information carefully so that recipients know where to find detail if and when needed. The person providing the information will not necessarily know who needs to receive it, or the timescale over which the information needs to be retained. Therefore, the use of corporate, rather then personal, storage is an essential part of good communication.

60. MOD systems and procedures offer many channels of communication, and maximum benefit will only be obtained by selecting and using wisely. The approach may depend on the urgency, whether a record needs to be kept, the level of security needed, the volume of material, whether the communication is to one person or many, bandwidth availability and other criteria. MOD systems should support both **information push** (as in speech, email, or telephone) and **pull** (as in a book or web site), the distinction being whether recipients are directly presented with the information or whether they need to seek it.

61. The MOD operates many computer-based Information Systems, and frequently needs to transfer information between them. Information also has to be exchanged with external organisations, including military allies, other government departments, commercial suppliers, and local organisations in theatres of operations. Although local initiative is often necessary to determine the most effective means of exchanging information between systems to meet immediate needs, there is benefit in using standard methods and protocols. The more widespread these become, the quicker, easier and, probably, cheaper it will be to exchange information reliably and securely between disparate systems.

62. There is continually growing demand for communications capacity to transmit higher volumes of information more rapidly, and for connectivity to share information securely and reliably with more partners; our systems should have the flexibility to expand.

63. Training, education and experience all help in good communication, as do standard procedures. Staff need to be proficient in use of **Plain English** in speech and writing, the guidance in the Defence Writing Guide (JSP101), and specific methods used to improve speed and efficiency of communication, such as formatted messages. The key to success is using a language that will be understood by the recipient.

64. Even where the initial communication was not in recorded form (for example direct speech), it may be necessary to take a record and store it in shared areas. This is a matter for judgement. Minutes of formal meetings are normally taken; even in informal meetings, a note (agreed by the parties) should be taken where significant decisions are taken, actions allocated, or where there is risk of misunderstanding.

Supporting Policy Statements - Policy Group 5

Communication of Information

65. The MOD will**:**

a. provide documentation and training on good communication and the supporting tools, accompanied by standard procedures (JSP 101 and others);

b. maintain and publish a set of information exchange standards (JSP 329, JSP 457, JSP 600);

c. require all of its computer-based information systems to adopt these information exchange standards (unless formally exempted by CIO).

Performance Monitoring - Policy Group 5

Communication of Information

66. The MOD will**:**

- independently assess accuracy, brevity and clarity of publications intended for broad readership across Defence;
- canvass opinion, and publish results, on the quality of communication of information received in a variety of forms;
- test its systems for compliance with information exchange standards.

POLICY GROUP 6

INFORMATION MANAGEMENT GOVERNANCE

67. Information in the MOD is a valuable asset, and needs to be actively managed as a corporate asset throughout its lifecycle. Therefore there must be a **mechanism to undertake this management**, both at the local level, and across Defence. There also needs to be an overall **policy governance structure**, setting IM policy, monitoring its effectiveness, adapting to business and technological change, and seeking continuous improvement.

68. The MOD's IM policy is determined by the Chief Information Officer. Because of the need for expert advice from across the MOD, and the requirement for coherence with other programmes, the department has a formal IM Policy Governance structure, reporting up to the Defence Board. For major IM policy issues, CIO will seek formal endorsement from a Steering Group comprising 1* TLB representatives.

69. **Management of information takes place 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):

a. the Senior Information Officer (**SIO**) is responsible for the Unit's information, sets local policy and procedures, and is accountable for quality;

b. the Information Manager (**IMgr**) is responsible for the implementation of IM within the Unit, issues local instructions, monitors performance, advises on information planning, manages necessary processes and information flows, and promotes IM awareness;

c. the Information Support Officer (**ISO**) is responsible for Information Administration, and is head of the Information Hub (iHub);

d. Information Administration functions are undertaken within the **iHub**. Tasks typically include; guaranteed action point for messages; maintenance of local file plan and team sites; permissions management; user account management; site collection management; provision of expertise in applications; storage of physical documents; liaison with system suppliers; advice to users. Posts within iHubs may have specific names, defining their role, or else will be called Information Support Administrators (**ISAs**), the collective term for all posts under the management of the ISO.

70. The wide diversity of Units, both fixed and deployed, means that variations from the standard are inevitable. Where there are local variations, these must be approved by TLBs - the Unit is responsible for ensuring that their local procedures meet the overall responsibilities of the specialist roles, and the tasks of the iHub.

Supporting Policy Statements - Policy Group 6

Information Management Governance

71. The MOD will**:**

a. publish the IM policy governance system;

b. establish a Steering Group to advise CIO on IM policy, and provide formal endorsement when needed, with representation from TLBs and MOD Centre Units;

c. mandate the roles of SIO, IMgr and ISO in all Units, and define what their tasks and responsibilities are, delegating to TLBs the task of how these roles are to be fulfilled;

d. mandate the iHub structure in all Units, and define its role, delegating to TLBs the method by which the iHub is implemented;

e. establish training for staff filling specialist IM roles, whether through separate courses or through incorporation into existing training packages.

Performance Monitoring - Policy Group 6

Information Management Governance

72. The MOD will**:**

- periodically review its IM Governance structure;
- undertake occasional assessments of individual iHubs to assess effectiveness.

POLICY GROUP 7

CULTURE, SKILLS AND PERSONAL RESPONSIBILITY

73. The MOD will benefit from a vigorous culture which encourages **responsible management of information by all staff, and personal initiative in its exploitation**. Good IM requires significant personal effort and discipline; sound training, documentation and procedures are also needed, as well as regular monitoring and reinforcement by local management. Effective exploitation will depend partly on how well the information is managed, but also on staff having a good knowledge of what information is likely to be found where, and how it can most readily be retrieved, as well as the ability to interpret many different sources of information quickly.

74. **Information Skills** are essential not just for those filling the professional IM and iHub roles, but for all staff (as well as other people who are regular users of MOD systems). They must be familiar with the principles of IM, the places where information can be found, and the methods of search and retrieval; they must also be diligent in administering any information under their control. Proficiency in use of the application software embedded with information infrastructures is also valuable. Having a wide variety, as well as depth, of information skills across MOD, is equally important. Good management and exploitation requires full engagement by all.

75. **Dedicated training courses** will be provided for staff filling specialist IM Roles. For other staff, Information Skills will progressively be incorporated within existing career and system-specific courses. Formal training will be augmented by widely available material for self-study or presentations by local staff.

76. **Sharing knowledge** and good practice, both locally and over information infrastructures, will enhance individual skills, and act as a spur to continuous improvement across Defence. The Information Maturity Model, a tool for self-assessment for individuals and Units, provides both a measure of, and a pointer towards the improvement in IM skills.

77. The NEC Competency Framework, an MOD extension to the UK standard Skills Framework for the Information Age (SFIA), codifies the skill set needed by MOD staff to exploit Network Enabled Capability, and covers both IM and Information Exploitation; it will in due course be absorbed into the overall competency frameworks.

78. There is now a substantial canon of **law applying to information**. Public Records legislation dates back over 150 years (though of course periodically updated), but most law is much more recent. Some relates to information access, both to restrict it (such as the Data Protection Act, and the Official Secrets Act), and to increase it (such as the Freedom of Information Act and Environmental Information Regulations). Other laws relate to behaviour while using information technology equipment, such as the Computer Misuse Act and the Malicious Communications Act. Other laws also embrace information, or information technology, within their overall scope (such as the Health and Safety at Work Act, the Disability Discrimination Act, and the Human Rights Act).

79. It is essential that the MOD complies with the law. Therefore we all need to have sufficient understanding of how legislation affects us in our handling of information. Any failure to comply may result in major embarrassment and cost to the department, and have disciplinary implications for individuals.

80. Personal responsibility involves:

a. assessing the importance, urgency and sensitivity of information;

b. working individually or collectively to ensure that the information is properly managed as a corporate asset and exploited;

c. ensuring that information that needs to be shared is communicated in the right way;

d. ensuring that information that needs to be kept confidential (for security or privacy reasons) is not inappropriately divulged;

e. recognising that mistakes can be made in handling information, and working cooperatively to correct errors and reduce risk of recurrence;

f. understanding how the individual user is affected by the law, complying with such law, and seeking professional advice as appropriate;

g. using MOD information technology in an appropriate way, and avoiding unacceptable use.

81. The department relies on the skills, aptitudes, abilities and motivation of the people who work for it. Its ability to exploit information to achieve its objectives depends on the collective desire and competence of its workforce and how well each member of the team manages information.

Supporting Policy Statements - Policy Group 7

Culture, Skills and Personal Responsibility

82. The MOD will**:**

a. appoint a senior champion to sponsor the people skills necessary for good information management and exploitation;

b. publish the key information management and exploitation competences;

c. provide training and education in Information Skills, either as dedicated courses or through incorporation into the syllabus of career courses;

d. encourage the inclusion of Information Skills in personal training plans;

e. promote Communities of Practice which seek to improve expertise and spread good ideas;

f. publish an IM Maturity Model;

g. publicise good practice, and, if necessary, salutary warnings;

h. instil a culture of personal responsibility for handling information throughout the Department;

i. maintain expertise on information law;

j. promote awareness of the key points of law relating to information handling;

k. maintain, publish and publicise an Acceptable Use Policy for MOD Information Technology and Telecommunications Equipment.

Performance Monitoring - Policy Group 7

Culture, Skills and Personal Responsibility

83. The MOD will**:**

- undertake routine internal and external validations of IM training;
- sample opinions of staff in IM specialist roles of the quality and relevance of IM training;
- plan and monitor the numbers of staff trained in specialist IM roles;
- promote feedback through the IM Community of Practice;
- periodically canvass a broad range of opinion on whether the level of personal responsibility in handling information is sufficient;
- periodically assess whether its understanding of the law is sufficient.

Annexes:

A. Introduction to the Information Management Protocols, Handbook and Maturity Model

B. Related MOD Documents

ANNEX A – INTRODUCTION TO THE INFORMATION MANAGEMENT PROTOCOLS, HANDBOOK AND MATURITY MODEL

THE INFORMATION MANAGEMENT PROTOCOLS

1. The policy defined in this document is reinforced by the **IM Protocols**. These provide concise guidance, and occasionally direction, to help people manage information better. Each protocol covers a single topic, is straightforward, and largely jargon-free. Protocols are generic, rather than specific to a particular computer system, and some of them are completely unrelated to IT. If used well, they should foster good standards of Information Management and Exploitation across Defence, and help people understand why IM is important.

2. The initial release contains about 40 Protocols, and there is scope to increase the quantity and the quality. All users will be encouraged to propose improvements to the existing protocols, and make suggestions for new ones. CIO will maintain the protocols based on this feedback, endeavouring to reflect and promote good practice.

3. The Protocols will be published on the Defence Intranet, together with the CIO contacts, and advice on how to contribute.

THE INFORMATION MANAGEMENT HANDBOOK

4. The **Information Management Handbook** was published by CIO J6 in 2006, with a foreword from VCDS and 2nd PUS. It sets out to establish a common and contemporary understanding of what information is, and why IM matters so much to all of us. It illustrates what happens when we do it well, and warns what might happen if we don't. It explains the key IM principles and concepts and how they fit together, and analyses the components of Information Management in detail. It explores ways of embedding IM within our daily work, and stresses the need for all of us to take responsibility for how we do it.

5. The Handbook is primarily aimed at people in staff appointments, for whom it is essential reading, but it is relevant to all of us who manage and use information. Those who read this document carefully will gain a good understanding of Information Management, and how we wish it to work within Defence. It places strong emphasis on the operational environments, while the good practice and guidance it offers are applicable throughout our business.

6. There is a précised version of the Handbook (the **Commander's Précis**) which offers a succinct, common understanding of IM to commanders, directors and team leaders across Defence.

THE INFORMATION MANAGEMENT MATURITY MODEL

7. The **IM Maturity Model** aims to provide a measure of how well a person or organisation understands and applies Information Management techniques. By assessing maturity, albeit fairly subjectively, people and organisations can understand where they need to improve, and which areas need most attention. The guidance needed can then be accessed from the Model.

8. The Model incorporates four surveys, each one designed for a specific audience and outcome: Information Managers, Team Leaders, Standard Users and Occasional Users. The survey seeks to assess, for each of a range of questions, the level of IM maturity of the respondent (from 'beginning' to 'excelling').

9. Completion of surveys should provide:
   a. Individuals with a summary of the essential elements of how to work with information;
   b. Local Command and Information Managers with an assessment of IM skills; and an indication of areas needing attention;
   c. MOD and TLBs & with an overview of IM skills, and issues that need to be resolved.

ANNEX B – RELATED MOD DOCUMENTS

10. For related documents see the Information Management Portal on the Defence Intranet (MOD personnel access only).