This edition of JSP 747 and its related documents has now been archived and is no longer published.

Policy

Managing and using information in Defence

Issue

Information is the lifeblood of Defence, both in military operations, and in all that we do to prepare for, and support, those operations. Information 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.

"Information" can cover both Data and Knowledge, as well as that which is held in recorded form, but which 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.

The better we use the information that is available, or potentially available, to us, the more effective we will be – that applies to us all individually, and it applies to Defence as a whole.

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.

Actions

For this policy to succeed, we need to develop and sustain the following 5 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.

This edition of JSP 747 and its related documents has now been archived and is no longer published.

Background

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.

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

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

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

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

For further information of how Defence collectively will follow its policy, and for what you should personally do if you work in Defence, see under the Detail tab.

This edition of JSP 747 and its related documents has now been archived and is no longer published.

Supporting Detail

Overall Policy

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.

This section contains

- What MOD collectively will aim to do – this is of interest mainly to policy staff and to information specialists;
- 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 everyone in Defence must do – this applies to us all.

What MOD collectively will do

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

- appoint a Chief Information Officer (CIO), to be the Defence Authority for the way in which information is handled;
- 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 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;

This edition of JSP 747 and its related documents has now been archived and is no longer published.

- 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.

For legal compliance, 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.

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;

To make information readily available to those who should have access to it, 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;

This edition of JSP 747 and its related documents has now been archived and is no longer published.

- 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.

To protect information securely from those who should not have access to it, 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 System Operating Procedures (SyOPs) for all MOD ICT services.

To preserve information for an appropriate period of time, 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 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

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

This edition of JSP 747 and its related documents has now been archived and is no longer published.

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;
- identify areas for improvement, whether in policy, guidance or practice, and inform the appropriate people;
- set a good example in all aspects of managing and using information.

What leaders and managers must do

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 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

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.

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 MOD CIO 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 things you know, 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;

This edition of JSP 747 and its related documents has now been archived and is no longer published.

- understand and follow 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 MOD for your job;
- follow the System 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 MOD's ICT or your own, or no ICT at all;
- know your local Information staff, and when in doubt, ask!