**Ministry of Defence Access to Information**

**Guidance Note**

Version 6 March 2009

## Guidance Note D1: What is Information?

### What is information?

1. The right of access applies to information recorded in any form. All recorded information that the MOD holds, in any permanent form, is potentially releasable under the FOI and EIR regimes **regardless of age or classification**. The information may be:

- in filing systems both paper and electronic
- on computers and IT networks including within email accounts, personal drives, removable media or other storage systems
- on video/audio tapes
- photographs, or maps
- plans, diagrams, or flowcharts
- in notebooks or logbooks or contained in wall charts etc

2. A key feature is that it is information **held,** not originated. It includes that received from third parties such as foreign governments, contractors, etc. These third parties do not have a veto on whether the information is disclosed. It is good practice to consult them, particularly where a qualified exemption applies and it is necessary to determine whether there are public interest reasons for withholding the information. In the following cases there is a requirement to consult:

➢ Separate arrangements have been made to consult third parties on Commercial information, you should read the separate Guidance Note on Commercial Information before responding to any requests for such information (Insert Link Here)

3. The information subject to the request is the relevant information that was held by the authority at **the time when the request** was received. There is no obligation to keep information which is not required for business or historic reasons; if the documents containing the requested information are destroyed before the request is received this is not contrary to the FOI Act or EIRs. BUT, once the request is received, relevant information may not be destroyed. If it is scheduled for destruction this must be postponed until the response is made, and consideration given to whether destruction is still appropriate.

4. The Act does provide that when responding to a request, an authority may take into account any amendment or deletion which would have been made to the recorded information in the normal course of events if it had not been in receipt of the request. **This provision should be used with great caution.** It is an offence to alter, deface, block, erase, destroy or conceal any item with the intention of preventing disclosure of any or all of the information to which the applicant is entitled. **An individual officer found guilty of this offence is liable, on conviction, to a fine of up to £5,000**. Following MOD rules and guidance will not expose staff to any risk of offence. However, failure to follow MOD rules could result in personal liability. A more helpful approach in responding to a request would be for the authority to be sure it has fulfilled its duty, under section 16 of the Act, to provide advice and assistance to the applicant. On occasion this may lead to information being disclosed which was described by the request but only received or recorded by the authority after the date on which the request was received.

The disposal of information contained in a structured system, such as registered files, must be in accordance with JSP 441.

- It is an offence to destroy information after a request for it has been received
- FOI requests, requested information and public interest test data should be kept for 5 years
- There is no requirement under FOIA or EIRs to create information in answer to a request.

FOI replies are on behalf of the MOD not your section or area. Be very sure to check everywhere before concluding that the information is not held.

5. The definition of "held" includes information **held by, or on the behalf of**, the department. Departmental records held in an external archive or registry, such as at the main MOD archive (run by TNT), are considered to be held by the owning TLB. When searching for information in response to a request for information it is the responsibility of the responding desk officer to obtain all the relevant information held by, or on behalf of, the MOD including archived files. See Guidance Note D8: Processes for handling a request for information.

6. **The FOI Act is classification blind**. Information bearing a protective marking is not automatically exempt from release, although this will indicate potential sensitivities and the possibility that an exemption may apply. See Guidance Note *A3.*

7. Information already in the public domain is exempt from requests under the general right of access (see Guidance Note C1: the MOD Publication Scheme). Information does not include non-existent information that could be created by manipulating existing information, although a digest or summary of this information may be created from existing data and provided in response to a RFI where this is reasonable under the duty to advice and assist. There is no obligation to include information that does not exist until further research has been carried out, although it would be helpful to indicate whether, and when, this might be available in the future.

8. The regimes give the right to obtain **access to the information itself and not to the document** or record, which contains it. The applicant is not expected to know the name or title of the record containing the information they are seeking. However, if a particular document is requested, this should be interpreted to mean that the applicant wishes to have access to all the information contained in the document. Only those parts of the document, which are exempt, may be withheld. The definition of **environmental information** in EIRs is very wide. A full description of environmental information is given in Guidance Note B3.

**Records Management**

9. The fact that the FOI Act and EIRs cover all information held by the MOD does not mean that we have to keep every document produced in the course of our work. But it is a criminal offence to destroy material once it has been requested. Good records management is a benefit, not a burden. The MOD already has clear records management procedures in place (see JSP 441).

9.1 **Retention and disposal** schedules form a key element to the MOD's records management policy. They are essentially timetables that set out when a business unit's records are not only due for review, but also when they should be considered for archiving or for destruction. These schedules enable the Department to establish in cases where records no longer exist, that they were disposed of in accordance with a proper decision making process. It follows that a record must be maintained showing which records have been disposed of under the schedule and when. Together, these measures will help to give the public confidence that the MOD has proper records management procedures in place.

9.2 A **document** is something that is written: which furnishes evidence or information on any subject. The significance of this definition becomes clear when viewed against the requirement to release 'information' on a specific subject or topic, in regard to the FOI Act. If a document contributes to a full understanding of a policy decision, or results in action being taken, or forms a significant part of the subject, it must be kept as a departmental record and, as such, will be deemed to be 'information' with regard to a FOI Act request for information.

9.3 There is no distinction between data recorded and conveyed on paper or electronically. All **e-mails** generated, or received, by members of a Department are public records and therefore are subject to Departmental records management policies and procedures. However, the fact that they are public records does not mean that they will be kept forever. Most e-mails will be

destroyed, some after a very short period, in accordance with standard record keeping procedures. If the sender or recipient of an e-mail decides it needs to be kept for more than a very short period, it must be filed in the MOD's official record keeping system.

9.4 Responsibility lies with both the originator of the e-mail and the recipient, for deciding whether an e-mail is to be retained. Both internal and external e-mails are legally recoverable evidence and, as such, care should be taken to ensure that they are free from unlawful, libellous, defamatory or inflammatory statements and ensure, as far as is reasonably possible, that the content is accurate and true and does not contain information that could prove embarrassing for the Department, should the information be made public. Above all, e-mails should be drafted with care and attention and nothing should be written that cannot be justified.

9.5 It is important to note that e-mails contained in personal mailboxes and deleted items boxes are potentially disclosable, either in part or whole, in response to a Subject Access Request, if they contain the relevant **personal** data. In general, once an e-mail is deleted, it is not deemed "held". However, on rare occasions, it may be thought reasonable to seek a copy from back-up systems.

**Unrecorded information**

10. The FOI Act does not apply to unrecorded information, except in two cases:

a) Under s.51 the Information Commissioner can require a public authority to furnish him with unrecorded information in the exercise of his investigative powers for the purposes of enforcing compliance with the Act. To do this, the Commissioner is required to issue an Information Notice to the public authority, specifying the basis for his request. He may also set the time frame for compliance with the Information Notice and the form in which the information should be provided. In practice, what this provision means is that the Commissioner has the right to request access to all information, including any unrecorded communication (e.g. oral briefings), to provide him with a full and complete understanding of the situation or decision taken. However, a public authority is not required to supply the Commissioner with certain information relating to communications between a legal advisor and client, or a person representing a client, about the client's compliance with the Act, or any proceedings arising from it.

b) Under s.75 the Secretary of State can amend or repeal other enactments, which prohibit the disclosure of information, including unrecorded information. An authority is not required to record information known to an officer or employee simply because a request has been received. However, if this information is held in recorded form by another person on behalf of the authority, then the right of access does apply.