Not to be communicated to anyone outside HM Service without authority

DCI GEN 97
1999

Defence Council Instructions

General

[redacted]

MINISTRY OF DEFENCE
9 April 1999

DCIs are automatically cancelled after one year

Contents

97/99 Use of the Internet

[D/DINFOD/22/3/2: [redacted]]

Purpose:

1. To state MOD policy on the use of the Internet and to ensure that all MOD publishing on the Internet is approved by the appropriate contact within the Defence Information Division (DINFOD).

Who should read it:

2. All MOD and Armed Forces personnel who deal with external contacts or who work in an area of public interest. All MOD and Armed Forces personnel who use or intend to use the Internet. All 1-star officers and equivalent and unit commanders.

Previous instructions replaced:

3. DCI **78/97**, (which replaced DCI **4/96**)

Other relevant information:

4. MOD Personnel Manual - Conduct under section 6, 'Disclosure of Information'.
JSP 440, Volume 1, Chapter 11 re. policy on the release of MOD information into the public domain.
JSP 406 and DCI **216/98** re. Data Protection Act 1998.
JSP 440 Volume 3 Chapter 24 re. Internet security policy.
Forthcoming DCI on 'The improper use of MOD's IT facilities'

Contact:

5. Directorate of Internal Communication & Media Training (DICMT) MOD Internet team on [redacted].

Contents

Introduction

7. The Internet is becoming an essential form of business communication. For the cost of a local phone call, it enables information to be transmitted rapidly across the globe to anyone with a computer, a modem and a telephone connection. It is also an increasingly important tool for research, public relations and promoting partnership with industry, particularly through the development of websites on the World Wide Web.

8. The Finance, Planning & Management Group directed that MOD's use of the Internet should be regulated to ensure that the opportunities it provides can be put to best use. Furthermore, a number of new Government-wide initiatives require all public sector organisations to examine how their use of the Internet can lead to better Government:

> *The Prime Minister's objective for 25% of all public dealings with Government to be capable of being conducted by electronic means by 2002.*
>
> *The Department of Trade and Industry's objective for 90% of central Government's routine purchases to be made electronically by 2001.*
>
> *The proposed introduction of a Freedom of Information Act to establish the public's right of access to Government information, subject to exemptions; the Internet provides the ideal medium to fulfil our obligations.*
>
> *The development of a Government Secure Intranet (GSI) to facilitate communication and information-sharing amongst Government Departments and provide access to the Internet*

A Developing a Business Case for Use of the Internet

9. It is essential that all MOD activities are regularly reviewed to consider whether a business case can be made for use of the Internet. This particularly applies to parts of the MOD with a large number of external contacts, or which attract public interest. Examples of potential benefits include:

- savings in information distribution costs e.g. printing, photocopying, packaging materials, staff time, postage;
- faster transmission of documents
- savings in storage and onward dissemination costs for documents received in electronic format;
- savings in staff time spent dealing with or redirecting enquiries;
- savings in staff time spent in researching information
- easier access to MOD information for the public, industry, other Government organisations both UK and abroad;
- good public relations.

10. Costs associated with use of the Internet include IT investment and staff time for acquiring appropriate skills, developing information materials and dealing with any resulting enquiries. Staff retention may also be a hidden cost. IT costs may be minimal, since it is not always necessary to have direct access to the Internet (this DCI will explain how the Defence Information Division (DINFOD) publishes information on the world-wide web for the MOD and single Services; it will also explain how the MOD Library Services can be used for Internet based research.) Internet access is required for those whose work involves direct correspondence with the public or with business, or those whose job effectiveness could be improved by interaction with the outside world via e-mail. Here there is a managerial cost in monitoring against time-wasting or misuse of the Internet by MOD staff (see forthcoming DCI on 'The improper use of MOD's IT facilities'). Although some guidance will be offered in this instruction for gaining an Internet connection, it is essential that MOD staff consult JSP 440 volume 3, chapter 24 for a comprehensive statement of MOD Internet security policy.

Publishing on the World Wide Web

11. The MOD and the single Services have well-established websites, managed by the Directorate of Internal Communication & Media Training (DICMT) and the three Service Directorates of Public Relations (DPRs) respectively. In general, DICMT oversees MOD and tn-service subjects and the DPRs deal with single Service public relations and recruiting. DICMT also has a wider responsibility for MOD policy on the use of the Internet.

12. The following examples demonstrate how MOD is already making use of the Internet:

Operations

At the outset of the Kosovo crisis in 1998 a special section was established on the MOD website in partnership with the Foreign Office. It provided key policy statements, detailed maps, photographs and up-to-the minute press notices. A similar initiative occurred during the Iragi crisis of late 1998.

Defence Policy

The Strategic Defence Review White Paper and all supporting material were published on the MOD website within minutes of the Secretary of State having presented it to Parliament. Nearly 300.000 accesses were recorded in the following 24 hours.

Recruitment

The single Service websites promote positive images of Service life to improve public relations and to attract recruits. The Army site has an 'Army Challenge' exercise which enables visitors to the website to determine whether they have the right instincts to become an officer and leads to an on-line application form. A significant proportion of Army Officers are now recruited via this route.

Defence Procurement

'Guidelines for industry', partnership creation information, the MOD Contracts Bulletin (subscription service) and Defence Standards are all available on-line.

13. These examples, however, represent only a fraction of the total business of the Department. At the time of writing, MOD is a long way from providing a comprehensive 'window to the world' of its activities. All the webmasters listed below welcome enquiries from anyone in MOD who wishes to publish information or provide services over the Internet.

Scope	Internet address	Contact	Telephone
MOD/ Tri-service	http://www.mod.uk	DICMT(IN)1	[redacted]
Navy	http://www.royal-navy.mod.uk	SIO(DPR)N	[redacted]
Army	http://www.army.mod.uk	DICMT(IN)2	[redacted]
RAF	http://www.raf.mod.uk	DPR(RAF) Sgt RAF Internet	[redacted]

14. It is recommended that anyone interested in establishing a presence on the web should first view the MOD and single Service websites to gain an impression of the type and scope of information currently available. It is also worth looking at other Government Departments, other Ministries/Departments of Defence and the websites of business contacts (see the MOD website's extensive links pages at *http://www.mod.uk/links/links.htm*). This should give a feel for the type of material best suited to the medium. High priority subjects for publishing on the Internet or delivering services via the Internet are as follows:

- where there is strong public interest in an area where your branch is responsible for policy, e.g. Gulf veterans' illnesses;
- where there is an opportunity to provide a service to the public e.g. Met Office weather forecasting service
- where the Internet offers more effective ways of doing business with external contacts, by giving access to publications, information databases and on-line forms e.g. procurement projects and the Public/Private Partnership Unit's pages on the Private Finance Initiative
- where there is an opportunity to promote the public image of MOD and the Armed Forces e.g. on-line versions of the Defence Estates Organisation's Sanctuary magazine and the Army's Soldier magazine.

15. The Internet may also be used for internal communication purposes, particularly where there is a geographically dispersed, or highly mobile community who do not have access to a common IT network. For example, the Army website is regarded as a tool for internal communications for the Army, the TA and soldiers' families. In general though, the Internet should not be used for branch or unit

websites, where the information is relevant or of interest only to an internal audience. These should only appear on internal networks or 'intranets'. The MOD Internet team liaise with a wide network of Intranet system managers to ensure that where possible, major announcements are also communicated to staff via internal IT networks.

16. After conducting initial research and identifying a business requirement to publish on the Internet, the appropriate webmaster in para.13 should be contacted. Provided the material is suitable, each will be able to offer advice or assistance in placing it on the Internet. The level of service on offer will depend upon the priority attached to the material, but will include some or all of the following:

Internet consultancy
advising how best to use the Internet as a communication medium, including advice on constructing web pages that the user can download quickly, avoiding mistakes that irritate web users (e.g. unnecessarily large images, redundant sound files etc.) and how to index pages in order to optimise detection by search engines.

Editorial
ensuring that the information is meaningful and interesting for an external audience.

Design
designing a web page or website, or offering design templates to allow information providers to design and update own website. For some requirements, such as intelligent forms, it may be necessary to engage external designers or programmers.

Web-hosting
providing free web space on a webserver with security protection to guard against tampering and facilities to record regular user access statistics (hit rates). In most cases, publishing on the webserver would be done by the webmaster.

Responsibilities of branches
17. The information owner or 'author' is responsible for providing material in an agreed format which meets the following *minimum* requirements for publication on the Internet:

- all material must be unclassified;
- all material must be approved by line management and should conform to the principles set out in MOD Personnel Manual - Conduct under section 6, 'Disclosure of Information'.
- no material should be published which could place MOD or Armed Forces personnel at risk

- all material of a scientific or technical nature must be approved by HQ Sy (ref: JSP 440, Volume 1, Chapter 11 policy on the release of MOD information into the public domain);
- all material must conform to the principles of the Data Protection Act 1998 (For further advice, contact MOD Data Protection Office on [redacted] or [redacted].)
- no material should be used where MOD does not own copyright and explicit permission has not been granted;
- no links to private sector companies that could be interpreted as an endorsement (although this does *not* preclude linking to a commercial website, for example in a page relating to activities such as a procurement project involving MOD and a partner or contractor);
- no links to any other organisations that could cause embarrassment to the Department;

18. Quality also means that MOD information on the web should be developed with the needs of the external user in mind. This principle must govern both the content and the design of the material. As a Government Department, the MOD is obliged to make its information available and comprehensible to the greatest possible number. This means that for all MOD information published on the web, and for the single Service sites where applicable:

- text should be written in plain English;
- it should not be necessary to understand the MOD organisation in order to access information about the MOD. In other words, the material should be organised by subject matter, rather than responsible branch. (An exception to this is where there is an established business requirement to promote a separate identity e.g. agencies);
- unexplained acronyms and jargon should be avoided;
- there should be a point of contact for further information;
- and most important of all, it must be up to date.

19. Authors should be aware, also, of the potential dangers of 'aggregation' when different branches publish related information and should factor this into their local assessment of whether information should be in the public domain. Advice on this can be obtained from the webmaster, who will have ultimate authority on the integrity, content and coherence of MOD information on the web. The author is also responsible for ensuring that material is accurate, up-to-date and unclassified. Information that is not updated according to the agreed frequency will be removed from the MOD webserver.

20. Where there is a business requirement to publish regularly on the Internet, it is recommended that branches develop web page authoring skills in-house. (Training can now be ordered through the MOD ICS Catalogue - customer support [redacted]). Branches who wish to develop their own web pages should conform to the

MOD design standards for publication on the Internet - see ANNEX. The same principles apply for single Service sites but the design and level of control exercised by DPRs vary, and advice should be sought from individual webmasters. If web pages provided by authors do not meet the required standards, the DINFOD webmasters reserve the right to modify the material provided prior to it being placed on the MOD or single Service websites. In the majority of cases, only technical modifications would be made. The author would be informed of any necessary changes prior to publication in case any further approval is required. It is strongly recommended that deadlines for web publishing take into account the need for DINFOD webmasters to check that web pages are at an acceptable technical standard and perform any necessary remedial work.

21. All MOD information on the web must be published on a web server with adequate protection against tampering; this means using the DINFOD contracted Servers, unless it can be demonstrated that the information is secure. Where the author has a business requirement to publish directly to the web server, either due to the volume of material or frequency of updates, it is possible to provide access to a sub-directory on the MOD server that can be accessed remotely. This requires prior approval by the MOD webmaster.

22. A checklist for branches seeking to publish material on the world-wide-web would be as follows:

- research material currently on MOD/Service websites and other relevant organisational websites
- draft publishing proposal
- contact relevant MOD/Service webm aster for advice, including how best to supply material and how publishing proposal fits into 'bigger picture' of MOD on the web
- develop material which must conform to all requirements for putting information in the public domain and obtain all necessary approvals
- deliver material in format agreed with webmaster and agree details of publication
- maintain currency of information and advise webmaster of any change of author responsible

23. As a general principle, any material which appears on the Internet should also be available to internal MOD audiences. The MOD Webmaster will be able to advise on how best to make information available via MODWEB to defence intranets.

Publicity materials

24. Publications which are published both on the Internet and in hard copy should, where possible, include details of how to obtain both versions - i.e. the electronic copy should contain an address from which a paper copy can be obtained and the paper copy should contain the address of the Internet version. The relevant

MOD/Service webmaster can advise on what this address is or will be. Associated publicity material (e.g. press notices) should likewise include the Internet address of the publication in question.

The Internet as a research tool
25. The quantity of information on the Internet continues to grow at an exponential rate. The World Wide Web offers a national and international, public and private sector perspective on issues and creates the potential for lateral approaches to problem solving. Other sources of information, such as Usenet discussion groups, can provide a potentially useful source of information. However, information on the Internet is of a highly variable quality. Researchers are advised to seek established and authoritative sources for mainstream research. In particular, it is advisable always to go to the original source for any article or publication to avoid the risk of getting a corrupted copy.

26. Most libraries in MOD act as centres of expertise and are equipped to conduct searches of the Internet. MOD staff can request searching to be undertaken on their behalf by information professionals skilled in retrieving information, or can arrange to use a library terminal for their own business-related research.

B. Accessing the Internet

27. It is essential that anyone wishing to gain access to the Internet first establishes with their network manager whether there is an existing strategy or timetable for gaining Internet access for their main business IT system. Some MOD IT networks operating at restricted level are moving toward gaining Internet access, either via the Government Secure Intranet or other means such as the Restricted LAN Interconnect initiative being developed by the Defence Communications Services Agency (DCSA). In the near future, this is likely to be only for exchanging e-mail, due to the security problems of gaining access to the World Wide Web, although this may be sufficient for a branch who can see a copy of their web pages on the intranet and simply need to be able to receive e-mail from the public. It is hoped that in the medium term full access to the Internet for both e-mail and browsing will be available from many MOD networks.

28. Within most areas of the MOD, full Internet access currently requires a standalone system which holds no protectively-marked or caveated material, a dedicated phone line and an account with an Internet Service Provider. Internet connections can be ordered through the MOD ICS Catalogue (customer support [redacted].) Branches should consider, when organising their Internet access, how best to monitor against misuse of the Internet. For example, some Internet Service Providers (lSPs) are able to provide audit trails. Commercially available 'net nanny' software can also be used to limit access to a predefined range of websites, e.g. pornographic sites.

29. In general, the appropriate sector IT security authority must approve all MOD IT systems. See the annexes to chapter 1 of JSP 440 Volume 3 for contact numbers of security authorities, as well as guidance and pro-formas for the preparation of system security policy and security operating procedures.

30. Gaining a connection to the Internet also requires prior approval from the sector Co-ordinating Installation Design Authority (CIDA) - see JSP 440, Volume 3, annex E to chapter 1 for contact numbers. The CIDA is concerned with the load on telecommunications networks and the security of the proposed installation, including the risk of TEMPEST (the leakage of electromagnetic radiation from computer equipment which could potentially compromise secure data on nearby machines). As a result of this approval process, it may be necessary to make changes to the physical layout of the office.

Use of Internet for e-mail

31. The Internet is, by its very nature, an insecure means of communication. It is essential that it is only used to send unclassified data, unless an approved encryption tool is used. Contact your local security authority for guidance on the use of the SECRETS for HMG which allows data to be sent up to restricted level. Under no circumstances should the Internet be used to send data at any level higher than RESTRICTED. For a full explanation of MOD Internet security policy, refer to JSP 440 Volume 3 Chapter 24. In case of doubt, contact the relevant sector IT security authorities referred to in para. 28 above.

32. Making it easier to communicate *may* have the effect of increasing the volume of communication. It is the line manager's responsibility to ensure that, when exchanging e-mail with external contacts or members of the public, the same standards of correspondence are maintained as for other written communication, particularly in terms of clarity of message, provision of an audit trail and minimum response times. All MOD Internet users should strive to ensure that the content of e-mail messages reflect a high level of professionalism and personal integrity.

E-mail addresses

33. When opening an Internet account for official business, MOD branches should use an official e-mail address. The only exception to this is where there is a need to preserve anonymity (although it should be stated that a non-official address does not represent any form of security). The MOD owns a Class A domain *(mod.uk)* which enables users to adopt a name of the form *xxxxxxxx@xxxxxxxxxx.xxx.xx*. In order to do this, it is necessary for you and your Internet Service Provider to obtain approval from the Defence Naming and Addressing Authority (DNADA) on [redacted]. Alternatively, MOD branches and Agencies may already have Internet connectivity through the Central Computer and Telecommunications Agency (CCTA), which owns the gov.uk domain. A *gov.uk* e-mail or Web address (e.g. *www.dera.gov.uk*) should, obviously, be regarded as 'official'.

ANNEX

Design standards for publishing MOD information on the Internet

DICMT and the three single Service DPRs are responsible for maintaining the quality of MOD's presence on the world-wide web. In addition to the minimum requirements for material published on the Internet (see para 17-18 of this DCI), MOD websites should conform to the following design standards:

- there should be a clear statement of permissible activity on all home pages to deter misuse (see wording on main MOD website)
- there should be a clear statement of Crown Copyright on all home pages (see wording on main MOD website)
- every home page should have a clear link to the main MOD or single Service site home page as appropriate;
- all subsequent pages must have a clear link to the home page;
- all pages should state when last updated;
- avoid unnecessarily large graphics - as a general rule, if an image is bigger than 50Kb it should be included as a separate file with a hyperlink;
- avoid use of sound files, except where absolutely essential;
- avoid use of web technologies which requires the user to obtain separate 'plug-in' software in order to read it (with the exception of Adobe Acrobat which is widely in use for providing exact copies of printed documents);
- where possible, avoiding use of 'frames' design which can not be read by some web browsers such as text-only browsers or those used by visibility-impaired people - at the very least, the top-level page should not be frames-based;
- avoiding use of any other web design features which require users to have one particular type or version of a browser;
- the information presented should in general be a credit to the MOD in terms of its overall look and feel

Detailed design guidelines for producing MOD web pages will be made available in due course.