

Policy on the use of IT facilities in the National Archives of Scotland

The purpose of this Code is to provide guidance on the use of desktop IT facilities, including e-mail and access to the World Wide Web. It outlines our policy on the personal use of the IT facilities and gives guidelines on what use is not acceptable. A range of communication facilities have over the last few years become available in NAS, including accessing the World Wide Web (Internet) and the use of internal and external e-mail. Used properly, these facilities can assist us significantly in improving our business performance and also help in the development of staff IT skills. It is very important, however, that we all behave responsibly when using these facilities.

Applicability

The code has been approved by NAS Management Board. This document applies to all users of NAS and SCAN systems, including individuals seconded to NAS and others (e.g. contractors) who might transmit information across departmental or public networks by means of e-mail or Internet services.

Responsibility

It is the responsibility of all users to comply with this Code. You must therefore ensure that you are familiar with its contents.

Personal Use of NAS Facilities

The purpose of NAS IT facilities is to enable you to carry out tasks which support the Department's businesses. It is important that you understand that the NAS owns and is liable not only for the equipment and material, but also for any e-mails and downloaded Internet pages generated or stored on NAS equipment. However, you may make limited personal use of the IT facilities in your own time, either when keyed out for staff on FWH, or outside normal working hours for those not on FWH. Personal use must also conform to the minimum standards of conduct as set out in this Code, specifically those detailed at paragraph 11 and at Appendix 1.

Permitted Personal Use

You may use NAS IT systems to prepare simple documents or spreadsheets on personal matters (for example a letter to your bank or insurance company or a social club contact list). Our registration under the Data Protection Act only covers information held on our systems for work related purposes, so personal documents should only be stored temporarily on our IT systems while they are being prepared, but must then be deleted.

You must not use NAS IT systems or the Internet to prepare or research material in connection with running a private business or any other material which could be held to be of direct financial benefit to you or any third party connected to or known by you. The Civil Service Code of Conduct applies to this provision.

If you are studying for any form of qualification, with Scottish Executive or NAS support, you may use the system to prepare study material. You must do this in your own time and ensure that you have the approval of your line manager.

Use of E-mail

You may send brief personal e-mails with small attachments to internal and external addresses, using the "message sensitivity" option in MS Outlook to mark such e-mails as "personal". For guidance, brief e-mails should be no more than 10 lines of text and small attachments should not exceed 2 pages. Please discourage the use of large incoming personal e-mails, particularly those with large attachments, as these can clog up the mail gateway and stop work-related e-mails being delivered promptly. You must not use official templates for personal documents. Private use of Chat Rooms and Newsgroups is not permitted. Management reserves the right to monitor e-mail activity including personal e-mails. Disciplinary action may be taken against any member of staff who makes improper or excessive use of the e-mail facility.

Internet Access

Accessing the World Wide Web for personal purposes is also permitted provided that you do so in your own time and do not act in any of the ways described in paragraph 11 below. If you are on FWH you must be keyed out of the FWH system. NAS monitors all Internet usage as outlined in paragraph 14 below. Line managers and Personnel will be alerted and disciplinary action taken if there is cause for concern about attempted access to inappropriate sites or excessive personal time spent on the Internet.

Misuse and unacceptable behaviour

If you misuse the system, you could be committing a criminal offence. E-mail is often spontaneous, which means that it can be written and issued without spending much time thinking about the content. However, if you make defamatory, actionable or untrue statements about colleagues or contacts on e-mail, it is no different from doing this in any other way. Such behaviour is likely to constitute a serious disciplinary offence and may also fall within the laws of libel. Guidance on legal issues is provided at Appendix 2. All messages must therefore reflect the high professional standards to which NAS subscribes. In addition, you must not seek to access Internet sites that are clearly inappropriate at any time.

A number of examples of what constitutes misuse of IT facilities and unacceptable behaviour are outlined below. This list is not exhaustive and each case is treated on its merits, but any of these may, depending on circumstances, be treated as misconduct liable to disciplinary action. Section A10.4 of the Staff Handbook - Discipline, contains details. Misconduct includes (but is not limited to) the following:

Attempting to gain or actively gain access to an inappropriate Internet site and obtain or attempt to obtain pornographic or other offensive material (e.g. racist material) and generate, store, distribute, or display such material. This includes similar items on official laptops, palmtops or electronic diaries brought into the workplace. An inappropriate site and offensive material includes content of a sexually explicit or sexually orientated nature; material that would offend others on the basis of race, religion, colour, sex, disability, national origin or sexual orientation; and, material relating to illegal activities or activities otherwise prohibited.

- Disclosing your private NAS password to someone else to use
- Loading any software for personal use onto your PC or laptop (for example screensavers, games, CDs from a computer magazine or shareware off the Internet). If you have any such software on your PC please remove it immediately.
- Subscribing to mailing lists ("list servers") through the Internet for purposes other than those that are work-related. This is to avoid unnecessary congestion of the e-mail system, and consequent delays to the delivery of official e-mail.
- Attempting to obtain access to parts of the NAS network, which you are not authorised to access, is a criminal offence. Gaining such access with the intention of modifying data or programs is a more serious criminal offence.
- Generating messages in a way that makes them appear to have come from someone else.
- Sending messages that are abusive, offensive, libellous or a nuisance.
- Generating and/or distributing chain e-mail.
- Using the IT facilities for private commercial activity.
- Contravening rules for personal use of IT facilities.
- Disseminating or printing copyright materials in violation of copyright laws.
- Getting involved in user groups or discussions which are politically sensitive or potentially controversial.
- Using the Internet for political activity.
- Running a personal website.
- Private use of chat rooms and Newsgroups
- Improper use of official templates
- Internet users can connect accidentally to Web sites that contain illegal or offensive material. If this happens to you, you should disconnect from the site immediately and inform your line manager. If you receive an e-mail that you consider may contain pornographic or offensive material, you should close the document, advise your line manager and inform a member of ICT branch staff.

Sensitive Data

Never send sensitive information, such as advice to Ministers, outside the Department in an external e-mail or over the Internet. The Government Secure Intranet (GSI) is currently the only vehicle to send mail to other Government departments for documents up to and including RESTRICTED, and at present NAS is not connected to the GSI. If you are in doubt about whether material is regarded as sensitive, please seek advice from a member of ICT branch about its transmission.

Monitoring use of the system

ICT branch staff are responsible for monitoring use of IT systems to ensure that security standards are complied with and compliance with this Code. All e-mail activity including traffic into or out of the NAS is logged. Similarly, a record is kept of every Internet site accessed, whether the attempt was successful or not. This record shows the originator's user name and PC, date, time and full site address of attempted access. You should be aware that many Internet sites keep a record of visitors to the site for marketing purposes and that this record could become public. You will need to ensure that you do not visit any sites where such publicity could lead to embarrassment to NAS. As part of standard monitoring procedures, baseline

information in the logs will be regularly examined. ICT branch will investigate any evidence of misuse.

Where there is evidence of misuse, the ICT Manager will report the matter to the attention of the Departmental Security Officer, who will decide in consultation with line management what action to take (see section A10.4 of the Staff Handbook - Discipline). Attempts to access, active accessing, downloading and transmission of pornographic, racist or offensive material will be treated as gross misconduct that could lead to dismissal. In extreme cases it may be necessary to involve the police, if there is prima facie evidence that a criminal offence has been committed.

If you believe that a colleague is misusing the system, or that your PC has been misused, you should contact a member of the ICT staff.

Compliance

You are required to familiarise and comply fully with the Code. You will be deemed to agree to its terms, including the monitoring arrangements, unless you specifically write to the contrary to Personnel Policy Unit, E1Spur, Saughton House.

Enquiries

If you have any enquiries about this Code, please contact the Departmental Security officer or ICT Manager.

APPENDIX 1 - GOOD PRACTICE GUIDE

1. The following guidance for network users (often called 'network etiquette', or 'netiquette') is based on advice provided to Internet users at sites around the world. It sets out what is considered acceptable behaviour. It applies to the use of e-mail, and any other electronic communications medium. It recognises that it is easy to despatch e-mail messages very quickly often without thinking how they will be received. For instance, if you have intended something in fun, will the humour be evident? If not, it could be offensive to those reading it.

Daily Routines and Housekeeping

2. You should observe the following good practice:

Check your e-mail regularly; ignoring a mail message is discourteous and can be confusing to the sender.

MS Outlook can send delivery receipts for e-mail - if you want to be able to check that your e-mail has arrived and been read, you should make use of this facility.

Don't assume that because you have sent a message, it will have been read.

Reply promptly. E-mail systems do not have the conventional 'pending' trays of the desktop, so it is easy to forget to deal with an e-mail message.

Treat the security of e-mail messages on the Internet in the same way as a message on a postcard (i.e. recognise that anyone along the chain of distribution could get to see what you have said, and it might even end up in someone else's hands). If you have sensitive messages to send to an external party, you must use a more secure medium.

Develop an orderly filing system for those e-mail messages you wish to keep. Regularly delete unwanted ones to conserve disk space.

Make use of the automatic reply system to advise that you will not be able to respond or who should be contacted in your absence.

Make arrangements for your e-mail to be forwarded to someone to handle when you are out of the office.

Ensure you give business contacts your correct e-mail address and include it on business cards and letterheads.

Writing Styles

Be careful how you express yourself. Remember that others than those for whom it is intended may read the message.

Try to keep messages fairly brief. Most people wouldn't choose a computer screen to read text on, in preference to a printed document, and it can get very tiring for some users. Try to restrict yourself to one or two screen-fulls at most.
Message Subjects

Make sure that the 'subject' field of your message is meaningful. Where someone receives many messages, it can be very confusing and frustrating not to be able to judge the subject matter correctly from its subject field. When you use the 'reply' option, ensure that the subject field (usually filled in for you under those circumstances) still accurately reflects the content of your message.

Don't broadcast e-mail messages unnecessarily. It's very easy to do, but can be very annoying to recipients (and wastes resources).

Other People's Messages

Don't make changes to someone else's message and pass it on without making it clear where you have made the changes.

Be 'Legal, Decent, Honest and Truthful

- Don't pretend you are someone else when sending mail.
- Don't send frivolous, abusive or defamatory messages. Apart from being discourteous or offensive, they may break the law and be subject to disciplinary action.
- Be tolerant of others' mistakes. Some people are new to this medium, and may not be good typists, or they may accidentally delete your message and ask you to resend it.

- Remember that the laws relating to written communications apply equally to e-mail messages, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information and wrongful discrimination.
- Remember that sending e-mail is similar to sending a letter on an official letterhead, so don't say anything that might discredit or bring embarrassment to the Department. This could lead to the matter being treated as a disciplinary offence.

APPENDIX 2 - LEGAL ISSUES

1. There is a wide range of legislation available to tackle the potential criminal and civil liability issues that may arise from employees' misuse of communication facilities while at work. Some of the key statutes are briefly discussed below.

Obscene Publications Act 1959

2. All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

3. A computer disk, including the principal hard disk of the computer, can constitute an obscene article for the purposes of this Act if it contains or embodies matter that meets the test of obscenity. 'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, and offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to be the originator or poster of the item.

Telecommunications Act 1984

4. The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under s.43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

Protection of Children Act 1978; Criminal Justice Act 1988

5. These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

Protection from Harassment Act 1997; Sex Discrimination Act 1975; Race Relations Act 1976

6. Harassment and discrimination are unlawful, whether or not the use of work-based communications facilities has played a role. Comments sent by e-mail are capable of amounting to harassment and of forming complaints of harassment and discrimination.

Data Protection Act 1998

7. Personal data as defined in the Data Protection Act, should not be included in any proposed Internet Web page, or other Internet entry, and care should be taken not to supply such information inadvertently if replying through e-mail.

Libel Laws

8. Information on the Internet is subject to libel laws. For instance in 1997 the Norwich Union was forced to make an out-of-court payment of £450,000 in damages to a rival private health insurer following misuse of its internal e-mail system by employees. Norwich Union's staff had circulated e-mail containing untrue rumours to the effect that another company was in financial difficulties and facing receivership. Items deleted on PCs are recoverable and defamatory material can be restored and used as evidence against a Department or individual.

9. In *Godfrey v Demon Internet Ltd*, the Court held that an Internet service provider was liable for a defamatory e-mail posted on its Usenet newsgroup because, even though it was not the publisher of the statement, it had failed to remove the statement as soon as it was informed that the statement was untrue. This meant that the Demon Internet Ltd knew that it had caused or contributed to the publication of the defamation, the defence provided by Demon did not succeed.

Copyright Laws

10. The use of material on the Internet is subject to similar copyright conditions as for other types of media. It is recommended that only a single copy of material is downloaded and that this copy is erased when the purpose for which it has been made has ended. Consent of the copyright holder should be sought if any large scale or systematic use of material is to be made. If it is proposed to incorporate material in a report, the permission of the copyright holder must first be sought and full attribution given. In recent years the software industry has taken determined action to protect its rights, forming organisations such as the Federation Against Software Theft (FAST), which has undertaken a number of successful legal actions.

Computer Misuse Act 1990

11. Introduced several criminal offences related to computers. As a result, it would be an offence for a person knowingly to obtain unauthorised access to the NAS Network, and a more serious offence to gain such access with the intention of modifying data or programmes and so impairing the operation of The NAS Network. The deliberate release of a virus is forbidden.