

**CSC 02/03
ICSC 01/03**

7 February 2003

File Reference A1550/01

TO ALL DEPARTMENTS

**NORTHERN IRELAND CIVIL SERVICE INTERNET AND E-MAIL
USAGE POLICY**

Introduction

1. This document sets out the policy of the Northern Ireland Civil Service (NICS) in relation to the use of Internet and e-mail facilities on departmental or agency Information and Communications Technology (ICT) resources. The policy applies to all NICS staff and others given permission to use departmental or agency resources to access Internet or e-mail facilities.
2. The policy also applies to the use of non-NICS equipment or facilities (including personal IT equipment at home or elsewhere) for the discharge of official business, for example, for work-related research or working from home. Individuals must not use non-NICS equipment or facilities for official business unless they have prior permission to do so. If permission is granted they must ensure that such use does not compromise the security of official data or expose NICS systems or equipment to risk of disruption from any source, such as a virus attack or unauthorised access. Staff should seek advice, as necessary, about IT security matters via their usual departmental IT contacts.
3. Internet and e-mail facilities can deliver significant business benefits and advantages when used appropriately and responsibly. However, careless or negligent use may waste resources and cause financial loss and damage to reputation. For example, unnecessary and/or unauthorised Internet/e-mail usage may cause network and server congestion, slow service delivery, reduce efficiency, consume supplies, and tie up shared resources. Also, misuse may lead to complaints or legal proceedings against NICS departments or individual members of staff.
4. The policy is intended to protect the interests of the NICS, as well as the interests of users, and to ensure that individuals are not at risk of disciplinary

action, criminal proceedings or civil action as a result of misunderstanding or lack of guidance.

5. All staff who use, or intend to use, NICS Internet or e-mail facilities for any purpose will be required to acknowledge that they have read, understood and will adhere to, the NICS policy and any related departmental or agency policies. Such undertakings should be renewed if the Internet and e-mail usage policies change. Failure to comply with the requirements of the NICS policy, and all other relevant departmental or agency policies, may result in disciplinary action – including dismissal.

Departmental/Agency Policies and Guidance

6. Where a department or agency has in place policies or procedures with more stringent conditions - such as restrictions on personal use of official equipment or on the use of non-NICS equipment or facilities for official business – such policies or procedures take precedence over the terms of this Circular.

Monitoring and Privacy

7. The Lawful Business Practice Regulations 2000 require employers to inform staff if there is a possibility that interceptions of communications might take place. Staff should note that, as is permitted by legislation, NICS departments and agencies will monitor and review Internet and e-mail activity, analyse usage patterns and may publish resultant data (traffic monitoring¹). Departments and agencies will also monitor the content of e-mails, files etc. as and when this is considered necessary in order to ensure the integrity of NICS systems and that users are complying with all relevant usage policies and guidance (content monitoring²). Use will be routinely monitored from time to time, and may be specifically monitored at any time when this is deemed necessary for compliance or other reasons, including the prevention or detection of illegal activities.

8. Users of NICS ICT resources, including Internet and e-mail facilities, should be aware, and must accept as a condition of use, that their usage of such facilities might be monitored and should have no expectation of privacy whether use is for the conduct of official business or for personal use.

1 **traffic monitoring** – recording and analysing websites visited, the addresses to which emails are sent, file transfers into and out of departmental/agency networks.etc. - the equivalent of recording the duration and destination of telephone calls.

2 **content monitoring** – looking at the actual content of e-mails, files etc. – the equivalent of recording and listening to the content of telephone calls.

9. Departments and agencies reserve the right to inspect and examine any and all IT equipment (including personally owned equipment) used on official premises, used for the conduct of official business, or connected in any way to the NICS Network, in order to ensure compliance with NICS, departmental, or agency Internet and e-mail usage policies. Therefore, users should clearly understand that if they bring into the workplace personal IT equipment of any nature, including laptop computers, or data storage devices such as floppy disks or CD ROMS, any such equipment or ancillaries, and data held thereon, may be inspected at any time to ensure that they do not pose a risk to the NICS whether by way of virus infection, hacking software or the presence of improper, offensive or illegal material.

Detailed Guidance

10. Detailed guidance is set out in the attached document entitled "Guidance on the Use of NICS Internet and E-mail Facilities". All users should familiarise themselves with its contents and should remember that the policy applies when using NICS resources for any purpose and also when using non-NICS resources (e.g. home computers/personal e-mail accounts) to conduct official business.

Consultation with Trade Union

11. The terms of this circular have been agreed with the Trade Union Side of the Central Whitley Council (for non-industrial civil servants). The industrial trade unions which formerly participated in the Central Joint Co-ordinating Council (for industrial staff) have also been consulted.

12. Any enquiries about the content or application of this circular should be addressed to your Establishment/Personnel Branch (NICS Code paragraph 1029 refers) or to your Establishment/Industrial Personnel Branch (NICS Industrial Code paragraph 400 refers).

AVIS BEATTIE
Employment Conditions and Pensions Division

GUIDANCE ON THE USE OF NICS INTERNET AND E-MAIL FACILITIES

Access to Facilities

1. Departments and agencies may make Internet and e-mail facilities available to staff for use in carrying out official duties. The decision as to which staff (or others) should have access to Internet or e-mail facilities is at the discretion of each department or agency. Departments and agencies may prevent connection of certain machines (holding sensitive data or applications) to the Internet or restrict use of Internet features such as file transfers, and will bar access to sites identified as containing inappropriate material.
2. Departments and agencies are responsible for the issue of User Ids and/or passwords to maintain individual accountability for Internet and e-mail usage. Individuals will be held responsible for the security of Ids and passwords.
3. Departments and agencies must ensure that facilities provided for e-mail and Internet access meet all relevant health & safety legislation.
4. Users must respect the privacy and legitimate rights of others, just as would be appropriate in any other work activity. Individuals will be held accountable for any misuse or breach of security, including confidentiality. Such misuse may lead to disciplinary action. Activities such as accessing, possession or dissemination of pornography or other offensive material, serious harassment or bullying, propagation of any virus or otherwise interfering with the integrity of NICS systems, or the possession of hacking software on official premises, are likely to result in dismissal. Where circumstances dictate, departments will inform and co-operate with relevant legal enforcement bodies.
5. Access to Internet and e-mail facilities may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected misuse.

General Responsibilities of Users

6. All of the usual NICS rules relating to conduct and normal standards of behaviour apply just as much when using Internet or e-mail facilities as at other times. Users must at all times conduct themselves responsibly and honestly when accessing the Internet or when using e-mail facilities. They must ensure that their actions do not:
 - a. waste time or resources;
 - b. expose the NICS network, or data held thereon, to risk of corruption, loss or inadvertent disclosure;
 - c. cause offence to colleagues or others;

- d. breach any law or statute; or
- e. otherwise bring the NICS into disrepute.

7. Unacceptable behaviour - such as harassment, bullying, dissemination of inappropriate material, offensive remarks or comments of a racial or sectarian nature, or regarding sexual orientation - is just as serious an offence if made in the course of using IT facilities as at any other time, and will not be tolerated. Inappropriate material may include, but is not limited to, any material of a pornographic, sexist, racist, sectarian, violent or offensive nature, whether in pictures, cartoons, words, sounds or moving images, and whether or not purporting to be of a humorous nature.

8. Users should note that they might be personally liable to prosecution, and open to claims for damages, should their actions be found to be in breach of the law. In cases of harassment, a claim by a user that he/she had not intended to harass or cause offence will not in itself constitute an acceptable defence.

9. Users should be aware that the possession of child pornography is a criminal offence. The NICS will fully co-operate with law enforcement authorities to identify and take action against any member of the NICS accessing, possessing or disseminating such material. Individuals found to have been involved in any way in the possession or dissemination of child pornography using NICS IT systems will face serious disciplinary action with a high probability of dismissal irrespective of whether or not they are prosecuted or convicted under the criminal law.

What Users May Do

10. Within this overall context users may (subject to the safeguards and conditions set out in this and any other relevant policy or guidance):-

- a. use e-mail to communicate with colleagues, customers, suppliers and other interested parties in carrying out their Civil Service duties;
- b. use the Internet to research relevant and potentially relevant information sources in carrying out their duties. In doing so, users may glean relevant information from trusted third parties (including news sites), provided prior approval for such access has been granted by local management; and
- c. participate (subject to local management approval) in officially sanctioned newsgroups or chat rooms in the course of business relevant to their duties. When so doing, users must not (unless specifically authorised to do so) speak or write in any department's name and must make it clear that their participation is as an individual speaking only for themselves. In any such use of Internet/e-mail facilities, users must identify themselves honestly, accurately and completely.

When participating in a chat forum or newsgroup users must:

- i. refrain from any political advocacy and from the unauthorised endorsement or appearance of endorsement of any commercial product or service;
- ii. give due regard to maintaining the clarity, consistency and integrity of the NICS, departmental or agency corporate image and avoid making any inferences that may prove inappropriate from a departmental, agency or NICS perspective;

and must not:

- iii. reveal protectively marked information, customer data, or any other material covered by departmental or agency policies and procedures; and,
- iv. use departmental/agency Internet facilities or computing resources to violate laws and regulations applicable in Northern Ireland in any way or to compromise the security (including confidentiality) of departmental/agency data.

What Users Must Do

11. At all times users must:-

- a. keep all passwords or user IDs confidential - the sharing of user IDs or passwords is prohibited;
- b. be alert to the risk of leaving an unattended machine logged on, which could lead to unauthorised use of their account and user ID;
- c. follow the security procedures approved for use with their system to ensure that any file downloaded from the Internet is scanned for viruses before it is accessed or run. Users who download such files, or who open attachments to e-mails, are responsible for ensuring that they are subjected to appropriate anti-virus scans (checking with the departmental IT Security Officer as necessary);
- d. report immediately any indication of virus or other attack;
- e. report immediately to their line manager or, if appropriate, to the departmental or agency head of Personnel, the receipt of inappropriate or offensive material delivered via e-mail;
- f. respect copyrights, software licensing rules and property rights, download only software with direct business use and do so in accordance with relevant departmental or agency policy; and
- g. as far as possible, schedule communication-intensive operations such as large file transfers, video downloads, mass e-mailings, etc. for off-peak times.

What Users Must Not Do

12. Users must not:-

- a. arrange to auto-forward e-mails from their Departmental account to personal e-mail accounts, or from their personal e-mail account to Departmental accounts. E-mails received into a Departmental account may be forwarded once their contents have been vetted to ensure that the forwarding of the e-mails does not contravene guidance in respect of protectively marked material;
- b. propagate any virus or programme designed to infiltrate a system (without the user's knowledge) to gather information (e.g. worm, Trojan horse) or other type of malicious program code;
- c. use any departmental or agency facilities to disable or overload any computer system or network, or attempt to disable, defeat or circumvent firewalls or any departmental or agency ICT security facility intended to protect the privacy or security of systems, networks or users;
- d. forward, send or store e-mails or other files containing inappropriate material;
- e. knowingly connect to any Internet site that contains inappropriate material. When such a site is inadvertently accessed, users will immediately disconnect from the site, regardless of whether that site had been previously deemed acceptable by any screening or rating program. Such inadvertent connections must be reported immediately to the relevant departmental or agency Help Desk so that appropriate action to bar access to the site can be taken and to safeguard the individual in the event of any subsequent investigation;
- f. use any departmental or agency systems or facilities to commit infractions such as harassment, unauthorised public speaking, misappropriation of intellectual property or misuse of departmental or agency assets or resources;
- g. intentionally access, archive, store, distribute, edit, record, or reproduce (on screen, hardcopy or via audio) any kind of inappropriate material on any departmental or agency system;
- h. use departmental or agency facilities to download and/or forward non-business related software or data including music, graphics, videos, text, games, entertainment or pirated software;
- i. use departmental or agency facilities to play internet games or forward chain letters (even in the user's own time);
- j. use departmental or agency facilities to participate in chat rooms, forums or newsgroups unless this is for business purposes and has been approved by line management;

k. upload any software licensed to a department or data owned by a department without the express authorisation of the manager responsible for the software or data;

l. transfer via the Internet (as opposed to the NICS Intranet) files containing RESTRICTED departmental or agency data unless the data is first encrypted using a product approved by the appropriate departmental or agency IT Security Officer. Files containing RESTRICTED material may be transferred via NICS Intranet. However, files containing departmental/agency data with a protective marking higher than RESTRICTED must NOT be transferred electronically. (Different rules apply in some cases – e.g. users of the OASIS system may transfer Confidential data to xGSI addresses. In such cases, users must comply with the appropriate departmental rules); and,

m. remain connected to the Internet while not actively using the resource.

PERSONAL USE

Definition

13. Personal use is defined as any use of Internet or e-mail facilities that does not stem from a requirement directly relating to the officer's official duties. Thus accessing a site for research purposes, for example researching social security policy or employment law developments, is official use only if such access is necessary as part of the officer's work. Accessing such data only out of personal interest, or to broaden general knowledge in that area, would be classed as personal use if the information is not actually required to discharge duties effectively.

14. Any access or use which is unrelated to official duties, for example, accessing general news sites, travel information, personal banking, sending or receiving personal e-mails and so on, would be classed as personal use.

Guidance on Personal Use

15. Departments and Agencies may permit staff to use official facilities for personal use, in their own time, providing that such use does not compromise the security of official data, result in increased costs or delays or have any negative impact on the NICS network or on the effective discharge of official business. Own time is when an individual is not on duty, such as before signing in or after signing out or during lunch or other officially sanctioned breaks. Individuals must apply for permission, in accordance with relevant departmental procedures, prior to undertaking personal use. The facility is granted at the discretion of management and may be withdrawn at any time for operational reasons, or if misuse is suspected or detected.

16. Users are reminded that all Internet and e-mail use is subject to monitoring. Such monitoring does not differentiate between official and personal use. Users should therefore ensure that anyone who may send personal e-mails, or other material, to their official e-mail address is aware

that the content of such emails may be monitored. Use of NICS facilities for personal use will be deemed as acceptance that usage, and on occasions, content, will be monitored.

17. Subject to departmental or agency policies in relation to personal use, users may in their own time:-

a. use Internet access for personal research, provided such use has been approved by local management;

b. use the Internet for the occasional purchase of goods and services, for example, books, flights, CDs, and so on, provided payment is made by the individual, and delivery of items purchased is to a private address. The user must not create any unauthorised contractual liability on the part of the NICS. The NICS does not accept any responsibility for the security of credit card details, or any other payment method used. Nor does the NICS accept any liability for financial loss, whether as a result of fraud or otherwise, suffered while using NICS systems for personal transactions. All such use is entirely at the individual's own risk;

c. make occasional use of departmental or agency facilities for on-line banking. All such use will be at the individuals own risk - departments cannot accept any liability for losses or for any other liabilities arising out of such transactions, howsoever caused; and,

d. make occasional use of departmental or agency e-mail accounts set up on their behalf, to send, forward or receive personal e-mails - subject to the conditions for using e-mail facilities set out in this policy. Personal e-mails must be clearly marked as being "personal". It is an explicit condition of using this facility that users accept that the content of such e-mails may be accessed, by management and/or IT staff, without notice or any requirement for further consent. While it is not intended to undertake routine monitoring of the contents of e-mails (personal or otherwise), e-mail traffic may be accessed at any time either as a result of checking an officer's e-mail account for business reasons if they are absent from work, or as part of an exercise to monitor compliance with internet and e-mail usage policy.

18. Users must not make excessive use of any of the above facilities to the detriment of their official duties.

Restrictions on Personal Use

19. Users must not:-

a. use departmental or agency Internet or e-mail facilities to carry out any activities for personal gain including, for example, share dealing or monitoring, investment portfolio management, or gambling; or

b. set up a personal e-mail account using departmental or agency resources unless prior approval to do so has been given by the Head of ISU.

Copyright and Similar Issues

20. Departments and agencies will, where it is deemed appropriate:-

a. retain the copyright to any departmental or agency material posted to any forum, newsgroup, chat room or World Wide Web page by users in the course of their duties; and,

b. assume ownership of any legitimate software or files downloaded via the Internet on to departmental/agency networks. Any such files or software may be used only in ways that are consistent with their related licenses and/or copyrights.