INTERNET POLICY

1 Introduction

1.1 Use of the Internet for the purpose of electronic mail is the subject of the E-Mail Policy. This policy covers use of the Internet to access information on third party websites and downloading of files from third party web sites.

1.2 This policy applies to staff who have direct access to the Internet.

1.3 The Internet is a global network of computers allowing information exchange across the world. Users are able to view and download information on a wide range of subjects and software. Staff can benefit in their work through appropriate access to the enormous store of information on the Internet. The aim of this policy is to encourage responsible and well-informed behaviour along with good management practice.

1.4 The guidance within this policy is intended to avoid staff placing themselves in positions where problems and legal issues can arise, particularly those related to harassment, defamation, copyright, entering contracts, pornography and official information. The guidance adds to, and does not alter existing staff rules in relation to the inappropriate use of CN4C resources, e.g. email and telephones.

1.5 Users of the Internet should be aware of the following associated risks:

- The difficulties of record-keeping and managing legal liability on electronic transactions.
- The internet is not a secure form of communication. Currently privacy and confidentiality are not guaranteed.
- The internet can be used to access inappropriate material.
- The problem of information overload when large quantities of information, some of which is of marginal value, is delivered to individuals.

2 Policy Statement

2.1 Access to the Internet will be provided and maintained by the Business Manager on the authority of the relevant Line Manager.

2.2 Access to the Internet is provided for use in connection with business purposes and for personal professional development in connection with the business of the organisation.

2.3 It is important that you read this policy and the accompanying appendices carefully before using or continuing to use Internet facilities. If there is anything that you do not understand, it is your responsibility to ask your line manager to explain it to you. Once you have read and understood the policy, you must sign the declaration at appendix 3 and send it to the HR Manager where it will be kept on your personal file. Staff who are unwilling to sign will not be allowed direct access to the Internet.

2.4 Occasional private use of the internet is permitted outside of working hours – i.e. during lunch breaks, or before/after work hours. It is for line managers to judge what is acceptable but excessive use which impacts on your performance is clearly unreasonable. Staff who abuse the system will have the facility withdrawn.

2.5 Although a huge amount of valuable information is now on-line, access to the Internet is open to misuse. In addition to problems of time management, specific issues can arise in relation to the retrieval and distribution of undesirable material. Individual use of the Internet will be monitored and all sites visited will be logged. Staff must not deliberately visit, view or download any material from any Web site containing illegal, pornographic, racist or sexist material.

2.6 The Organisation will place constraints on the use of the Internet to protect its legal position with respect to Data Protection, copyright and contractual law, to ensure the confidentiality of communications and the protection of privacy, to comply with record keeping requirements and to implement other Organisation policies.

2.7 Breach of this policy will result in appropriate disciplinary action.

3 Guidance on Use of the Internet

3.1 All staff who have signed the declaration at Appendix 3 below may access Internet web sites directly. This includes visiting sites, printing pages and downloading documents and files using the browser. There is a wealth of useful information on various sites in relation to the business, but before attempting to use the Internet for research, you must read the guidance.

3.2 You can print web pages and download documents and files using the browser - as long as these are not executable files (programmes) or encrypted files - although you may not be able to access certain types of unsuitable or secure sites and services. You must refer to this guidance on how to use the Internet properly and effectively.

3.3 Information from the Internet needs to be viewed and used with caution. Unlike traditional commercial information channels where contracts and liabilities ensure quality, there are no such controls on the Internet and consequently verification of sources is necessary. Information may not be current, complete or accurate and is also subject to copyright and established libel laws.

3.4 What you should do

The Internet is available primarily for business purposes, however:

- Occasional and reasonable personal use of the Internet is permitted outside main working hours, as long as this does not interfere with the performance of your duties or slow down the system for other users.
- Should you inadvertently find yourself at an Internet site with inappropriate or offensive material, disconnect from the site immediately and let your line manager know.

What you should not do

You should not:

- Visit, view or download any material from any Web site that contains illegal and/or pornographic, racist or sexist material.
- Subscribe to any bulletin boards, news companies or any other Internet service without prior written agreement from your line manager and the IT Manager.
- Allow those without access to use your computer in order to gain access to the Internet.
- Assume information on the Internet is accurate, complete, valid or up to date.
- Download software onto the Company's system. This includes software and shareware available free of charge from the Internet.
- Spend long periods of time on line (e.g. playing virtual golf against members of retirement communities in Arizona).

4. Monitoring

4.1 Use of the Internet will generally be subject to regulation consistent with all relevant legislation and CN4C policy and guidelines. Self-regulation will be encouraged and the organisation will impose limits or take action only where and when necessary.

4.2 You should be aware that CN4C may monitor and audit the use of the Internet. We will respect your privacy as far as possible, but messages and information you send or receive will be recorded and may be inspected.

4.3 You should also be aware that items deleted on PCs are recoverable, and unsuitable material can be restored and used as evidence against an individual or the organisation. Failure to comply with this guidance may therefore result in:

- disciplinary action being taken against you which, depending on the gravity of the offence, may be considered gross misconduct; or
- legal claims against you and/or the organisation (see appendix 1)

APPENDIX 1: LEGAL IMPLICATIONS

You should be aware of the following Acts of Parliament that are in place to protect both yourself, and the Company.

4.3.1 The Data Protection Act 1998

The Act requires organisations to process computerised personal data fairly. Auditing of e-mail or Internet usage falls into two main companies:

- logging/ monitoring of use; and
- inspecting the actual content of e-mails and Internet sites visited or downloaded.

The 1998 Act does not prohibit pre-announced routine audits or targeted audits in either category. However, there must be a good reason, such as cost control, suspicion of unlawful acts or defamation, copyright infringement and harassment. Therefore auditing is acceptable if carried out as a part of a published policy, as long as users are advised in advance. This is what the Company is doing by issuing this guidance and asking you to sign a declaration.

In relation to monitoring of e-mail contents, an organisation is entitled to monitor the content of work-related e-mail and Internet usage to reduce employer liability for employee action and to prevent abuse of equipment.

Monitoring the content of personal e-mail/Internet usage is a more involved issue. If an employee does not consent to this then the organisation will certainly contravene the data protection legislation and breach the implied duty of trust and respect within the contract of employment. Signing the acknowledgement form in appendix 3 is deemed to give this consent. As noted in the text above, the Company will not examine the content of e-mails unless there are good reasons to suspect the system is being abused.

In principle, the Act allows an employee to access any personal data collected by an audit.

4.3.2 Human Rights Act 1998

The present Government's commitment to incorporating the European Convention on Human Rights into domestic law has led to the introduction of the Human Rights Act 1998. This Act which, amongst other things, covers the right to privacy, came into force in 2000. A UK citizen will be able to assert their Convention rights through the national courts without having to take their cases to the European Court of Human Rights.

4.3.3 Telecommunications Act 1984

The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under this Act.

4.3.4 Obscene Publications Act 1959

All computer material is subject to the conditions of this Act. Under this Act 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.

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, offering for sale of for lease. It seems clear that material posted to a news company or published on the 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.

4.3.5 Protection of Children Act 1978: Criminal Justice Act 1988

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.

4.3.6 Protection from Harassment Act 1997: Sex Discrimination Act 1975: Race Relations Act 1976

Harassment and discrimination are unlawful, whether or not the use of work-based communications facilities have played a role.

APPENDIX 2: GLOSSARY OF COMPUTER JARGON TERMS

Address: Either the address of a user of a system, as in an e-mail address or the address of a site on the Internet.

Gateway: A computer system which transfers data between networks.

GSX: One of the Government secure intranets.

Hit: An entry on the log file of a web server. A hit is generated by every request made to a web server.

HTML: HyperText Markup Language

Hyperlink: Clicking on a hyperlink will take you to a linked page (usually referred to as 'the link') which can be on any site anywhere on the World Wide Web. Hyperlinks often appear as underlined key words on a Web page.

HyperText Transfer Protocol (HTTP): This is the most commonly used method of transferring information across the Web and presented to the user when it arrives.

Internet Protocol (IP): The mechanism for controlling the data which follows across the Internet.

IP Address: The IP Address is a unique identifier that can be used to locate the computer that sent a particular e-mail or visited Web site.

Search Engine: A database of information which links to certain key words, when queried by users. Internet users can use this data to find the information required.

Uniform Resource Locator (URL): This system attempts to standardise the location or address of a Web site, e.g. http://www.

Web Page: A section of information accessed by a user.

Web Server: A computer which hosts one or many Web sites and is permanently connected to the Internet.

Web Site: A company of linked Web pages.

World Wide Web (www): A hypertext based information and resource system for the Internet.

XML: eXtensible Markup language - a modernised version of HTML.

APPENDIX 3: ACCEPTANCE BY MEMBER OF STAFF/BOARD MEMBER/VOLUNTEER

I have read and understood the above Internet policy and undertake to act within it. I understand that the Company may monitor my use of the Internet and may inspect the content of Web pages visited.

I also understand that breaches of this policy will lead to disciplinary action in accordance with the Company's Disciplinary and Grievance Procedures and/or legal claims being made against me.

Name: .....

Job Title:.....

Signed: ……

Date: .....