HARBOROUGH DISTRICT COUNCIL

DISTRICT OF HARBOROUGH

INFORMATION AND COMMUNICATION TECHNOLOGY

INTERNET USAGE POLICY

Version 7.0 October, 2011
Peter Rowbotham - Head of Customer and Community Services

Contents

1. Introduction

The Internet is used by HDC to obtain information, research particular topics, transfer information to and from other organisations, etc. All staff and elected members with access to the corporate ICT systems have access to the internet.

The purpose of this document is to provide advice to staff and elected members on accessing the Internet.

2. Provision of Access

For staff members to have access to the Council's ICT systems a new user request form must be completed electronically and submitted to ICT Services by the appropriate Service Area Manager.

For elected members to have access to the Council's ICT systems a new user request from must be completed and submitted to ICT Services by a member of Management Board or the Head of Customer and Community Services.

3. Limits on usage

To encourage staff to increase their IT skills and knowledge, the Council allows moderate access by staff to the Internet for personal use. Personal access should be during the lunch break or outside the person's normal working hours i.e. they should have 'clocked out'. Personal use of the Internet is subject to review by the Service Area Manager and can be restricted or withdrawn if this is thought appropriate. Access to the Internet for personal use must conform to section 4 below.

The Council will monitor Internet traffic and internet sites visited, and periodic reports will be produced and distributed to Service Area Managers. The monitoring reports will also be subject to Audit scrutiny.

4. Prohibited Activities

4.1 Downloading Software

Although software is available for download on the Internet, users must not download software because of the risk of introducing viruses and unauthorised software to our network. There are also licensing and copyright implications. Any software which is to be downloaded from the Internet must be performed by ICT Services staff.

4.2 Misuse

Users should not use or try to use Council provided Internet access for any of the following purposes:

- Breaking through security controls, whether on the Council's network or any other computer system.
- Accessing Internet traffic (such as e-mails), whether or not protected by security controls, not intended for that user, or doing anything, which would adversely affect the ability of other authorised users to access the Internet resources.
- Intentionally accessing or transmitting computer viruses or similar software.
- Intentionally accessing or transmitting information about or software designed for breaching security controls or creating computer viruses or similar software.
- Intentionally accessing or transmitting material which is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represent values which are contrary to Council policy.
- Knowingly doing anything which is illegal.
- Private business.
- Any deliberate activities which would cause congestion and disruption of networks and systems.

The Council reserves the right to:

- Withdraw the users' right to any computer systems, access to networks, and communication services including the Internet.
- Prohibit access to certain specific content, web pages and other Internet resources.
- Remove or substitute the hardware or software used to access the Internet, at any time and for any reason.

5. Consequences of violations of the Council's Internet Policies

5.1 Staff

The Council will respond to violations of the above policies by any combination of:

- Informal warning.
- Withdrawal of Internet facilities for a period of time or permanently.
- Invoking the Council's formal disciplinary procedures.
- Seeking reimbursement of costs incurred by the Council.
- In appropriate cases, the provision of information to the police for possible criminal proceedings.

5.2 Elected Members

Any breaches of this policy by elected members will be referred to the Standards Committee for appropriate action.

6. Publishing Information on the Internet

The appropriate Service Area Manager will be responsible for the accuracy of information about their service published on the Internet. The responsible Service Area Manager may not be the author of information contained in a web page but the officer must ensure that the information is produced or provided by an expert in that subject and concerns activities within their authority, expertise and competence.

Information must be kept up to date and topical, and any links to related web pages must also be kept up to date.

7. Quality of Information available from the Internet

Information available from the Internet is of very variable quality and should not be relied upon uncritically. It is the responsibility of the user to make judgements about any information obtained from the Internet. For example information published on Government web pages or by other local authorities is likely to be of higher quality and be more accurate and reliable than information published on someone's personal web page. The user must decide whether the information is good enough for the purpose for which it will be used and if necessary verify it independently.

8. Viruses

It is a crime under the Computer Misuse Act 1990 to deliberately introduce a damaging virus. AntiVirus software is used on the Council's network but new viruses are always being introduced and although AntiVirus software is constantly updated, there is always a threat that a virus may be introduced by downloading files from the Internet, receiving e-mail attachments etc.

If a user believes they have inadvertently accessed material which may contain a computer virus, the user should stop using the computer and contact the ICT HelpDesk on extension 1313 (full number 01858 821313) for further advice.

9. Copyright Infringement

The main risk of copyright infringement is through users downloading files from the Internet. Copyright infringement can also occur where text is copied or attached to an e-mail. Equally users must not transmit copyright software from their computer to the Internet or permit anyone else to access it on their computer via the Internet.

Users should not copy information generated by others and re-post it without permission of the author, or at least acknowledgement of the original source, even if the content is modified to some extent.

Copyright and other rights in all messages posted to the Internet from a Council account, like other material – including intellectual works – produced at work belong to the Council and not to the users' personally.

Users should not assume that information posted to the Internet actually originates from the person or organisation that appears to have produced it, without some form of independent verification.

Copyright infringements may have severe cost implications for the Council.

6. Further Help

If you require further help or assistance with the content and requirements of this policy please contact ICT Services on extension 1313.