

Internet Usage Policy

Name: Corporate Internet usage policy

Version: 1.5

Issue Date: 22/07/2003



File	Internet Usage Policy	Page	1	Version	Version 1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Document Control

This is a CONTROLLED document and updates or changes to this document are authorized and then advised by email to the relevant document holders.

It is UNCONTROLLED when printed. You should verify that you have the most current issue.

DOCUMENT HISTORY

Author(s)

Names	Role
John Pritchard	ICT Enterprise Architecture Manager

Document Log

Version	Status	Date Issued	Description of Change	Pages affected	Review
1.0		22/07/2003	Approved and adopted by the Chief Executive Management Team (CXMT).		
1.1	Final	11/10/2007	Review & Updated	All	October 2008
1.2	Final	20/10/2008	Reviewed	All	October 2009
1.3	Final	11/01/2009	Reviewed	All	October 2010
1.4	Final	11/05/2010	Removed ISO9001 Logo	All	April 2011
1.5	Final	15/06/2011	Reviewed	All	May 2012

File	Internet Usage Policy	Page	2	Version	Version 1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Contents

1. Introduction	4
2. Aim.....	4
3. Within scope	5
5. Permitted and Prohibited Uses	5
6. External Connections	5
7. Breaches of Security	6
8. Conditions of Use.....	6
9. E-mail access through the Internet	7
10. Virus Controls	7
11. A Guide to the Legal Issues Relating to Access to the Internet.....	8
12. Software Copyright	8
13. Monitoring	8
14. Modification.....	8

File	Internet Usage Policy	Page	3	Version	Version 1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

1. Introduction

Whilst the Council's connection to the Internet offers numerous potential benefits, it can also open the door to some significant risks to data and systems, if users do not follow appropriate security discipline. Users may be held accountable for any breaches of security or confidentiality resulting from their use of the Council's Internet connection.

The overriding principle is that information security is everyone's responsibility.

Unnecessary or unauthorised Internet access causes network and server congestion. It slows other users, takes away from work time, consumes supplies and ties up printers and other shared resources. Unlawful Internet access may also result in negative publicity for the Council and subsequent exposure to significant legal liabilities.

The Council expects users to use Internet access primarily for business-related purposes to communicate with partner agencies, to research relevant topics and obtain useful business information (except as outlined below). The Council insists that users conduct themselves honestly and appropriately on the Internet and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, as in any other business dealings.

Any breach of the rules in this Policy by any user could result in disciplinary action being taken that could lead to dismissal. Misuse or breach of the Policy could also lead to civil or criminal actions against the user and/or the Council.

It is essential that all Council Internet users read this policy. Breaches of this policy will be taken very seriously. Any user requiring an explanation of this policy should contact their line manager in the first instance.

2. Aim

The Council views access to the Internet as a tool to aid employees in their job. However, the use of this tool can expose the Council to technical and legal risks if it is not used sensibly. The aim of this policy document is:

- To inform employees of the Council's policy on Internet usage to minimise the Council's exposure to these risks;
- Explain to users what can and cannot be done;
- To inform users of the legal risks taken whilst using the Council's Internet facilities;
- To inform users of the possible consequences for both users and the Council if this policy is not adhered to.

File	Internet Usage Policy	Page	4	Version	Version 1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

3. Scope

3.1 Within scope

All users granted access to the Internet by Herefordshire Council.

Any member of staff, whilst representing the council, using internet facilities provided by another organisation.

3.2 Out of Scope

Individuals not using Internet facilities provided by Herefordshire Council, as long as they are not representing the council and using internet facilities provided by another organisation.

4. Personal Use

Whilst Internet facilities are provided primarily for official council work, it is appropriate for employees to make **reasonable** use of the facilities for non-official purposes subject to the conditions set out in this policy.

The interpretation of what may be considered as reasonable or unreasonable is to some degree subjective and occasions may arise where an individual may perceive a different view from colleagues or supervisors. It is the responsibility of the user to take any necessary steps to clarify the situation or to seek permission from their Head of Service before using the facilities.

It is not the intention of the Council to place excessive obstacles in the way of users to prevent them from using facilities. All that is asked is that reason and prudent judgement is applied before proceeding.

Reasonable personal use is defined as but not limited to outside of working hours, for example before and after work and lunchtime.

5. Permitted and Prohibited Uses

Employees may use the Council's Internet access facilities for Council use subject to the rules in this policy. Employees may also use the Internet access facilities for personal use provided that such use is either within lunch or designated break times or outside core hours and kept to a reasonable level and does not interfere with business efficiency. Personal use of the internet which may involve any risk to the Council or its employees, through civil or criminal action, or which may bring the Council into disrepute, is not permitted. Any personal use of the internet facilities will be the responsibility of that individual. All risk associated and any loss incurred by the individual will be their sole responsibility and not that of the Council.

6. External Connections

The Council Internet gateway service provides secure access to the Internet from desktop personal computers.

File	Internet Usage Policy	Page	5	Version	Version 1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Using a 'firewall' between the Council internal network and the Internet provides primary security; bypassing the firewall is therefore **not permitted**. In some cases, individual external connections are permitted. In these cases, the machine used for external access **must never** be connected to any internal Council network. By using any external connections from Council equipment, users indicate that they will comply with this policy. All users of external connections must obtain prior authorisation to do so by ICT Services who will specify limitations on use and assess all risks associated with the usage.

7. Breaches of Security

Any breach of this policy will be dealt with as set out in the 'Information security Incident reporting procedure' which may lead to disciplinary action and possible termination of employment. Illegal activities may also be reported to the appropriate authorities.

8. Conditions of Use

- All risks associated with usage of the Internet must be assessed before using the service. Lack of confidentiality, integrity and availability must be considered, as the Internet provides no guarantees in these areas.
- No user may use the Council's Internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- Sharing of user names and passwords is not permitted unless prior agreement has been obtained from the Information Security Section.
- Employees must ensure that they are logged off from Council systems and the Internet when they leave the office or when leaving their computer unattended.
- Any licence conditions relating to the commercial use of software available on the Internet must be observed.
- Employees must not transfer files or programmes to or from unauthorised external sources via attachments, which may hinder damage or disrupt the operation of any application or a user's system software and hardware.
- No software program or script should be downloaded from the Internet by any user, unless with prior approval from ICT Services. In any event, entertainment software (e.g. Music, games, screen savers, ring tones etc) will not be approved.
- Copyrighted laws must be conformed to.
- All users are reminded that internet chat rooms and newsgroups are public forums where it is inappropriate to reveal Council confidential information, customer data and any other material covered by other existing Council policies and procedures.
- There must be no reference to the role of any individual or their duties within these types of site.
- No users should buy or sell goods or services via the Internet, unless they are officially authorised to do so or on behalf of the Council in accordance with documented policies and procedures as such transactions could bind the Council. If doing so they must use a Corporate Credit card with pre approval for any purchases.
- You must never use your Council email account to join websites or purchase good for personal reasons. You may use the Councils internet connection to purchase goods and services in your own time using your own personal credit card.

File	Internet Usage Policy	Page	6	Version	Version 1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

- This is at your own risk and the Council accepts no liability for loss from insecure websites or Council infrastructure.

9. E-mail access through the Internet

- E-mail is defined in two ways in this context: communications with people outside Herefordshire Council using a user's council e-mail address (a.n.other@herefordshire.gov.uk, etc), and private e-mail accounts (hotmail, etc)
- E-mail must not contain indecent, obscene or libellous material, material likely to cause offence or any material which harasses any other employee or third party on the basis of sex, race or disability or any other areas mentioned in the Council's Corporate Equal Opportunity's Policy:
- Email users must not send or deliberately attempt to receive e-mail known to contain a virus or malware.
- Email users must not use e-mail for gambling, conducting illegal activities or soliciting for personal profit.
- Email users must not reveal or publicise information, which is confidential either to the Council or its customers and clients.
- E-mail chain letters or virus hoaxes must not be forwarded. If there is any doubt about the nature of any correspondence received by a user then that user should consult the ICT Services Helpdesk immediately on ext: 0160.
- Email users may not access the internet using the logon credentials of another user.
- Email users must not send official information by Internet e-mail, such as Gmail or hotmail.
- Email user must only use an @herefordshire.gov.uk account to purchase good on behalf of the Council.
- Scanned signatures **must not** be attached to Internet e-mails. Such signatures can be disseminated by recipients and fraudulently attached to other documents purportedly in the name of the Council.
- E-mail attachments should not be opened unless the recipient knows whom they are from or is expecting to receive them.
- It is possible for e-mail messages sent via the Internet to be accessed by people other than the intended recipient. It should therefore only be used for information which is not commercially sensitive or covered by the Data Protection Act (1998), see the classification guidelines for further detail about what information can be sent.

Before forwarding e-mail to a new recipient, make sure you read the entire earlier messages, as they could contain personal comments that should not be redistributed.

10. Virus Controls

Up to date corporate anti-virus software must be installed and active on all PCs. No user should attempt to disable this software.

All electronic information received by the Council must be checked for viruses. This includes all floppy disks, CDs, e-mail, optical disks and removable media.

File	Internet Usage Policy	Page	7	Version	Version 1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

11. A Guide to the Legal Issues Relating to Access to the Internet

Employees are not to use the Council's Internet facility to engage in activities that are of questionable legality (at any time), that might harm the Council's reputation or that might otherwise violate Council policy such as:

- Peer to peer file sharing sites
- Online Gambling
- Accessing, displaying or disseminating pornography.
- Posting information that may tend to disparage or harass others on the basis of gender, race, age, disability, religion, sexual orientation or national origin.
- Participating in chain letters.
- The use of anonymizer web sites
- Posting statements that are defamatory or information that is false or misleading concerning the Council or any other organisation.
- Posting confidential or proprietary information about the Council, or any of its partner agencies or associates, on Internet sites.
- The Council accepts no liability for personal lose of our internet facilities, for example where you have purchased good online and you credit card details are stolen.

12. Software Copyright

Copies of licensed software must not be made without authorisation. In any event, software theft is illegal.

Software should not be downloaded or used unless a business case is submitted and approval received from the Information Policy Group.

13. Monitoring

A reporting tool has been installed to monitor activity on the Internet. The software logs information regarding user name, date, time, and site visited. Continuous monitoring of the logs will provide future advice to management on appropriate filtering of sites. The Council reserves the right to inspect all files stored in private areas on their network and personal computers at any time, without notice, in order to assure compliance with policy.

Sexually explicit or offensive material may not be displayed, archived, stored, distributed, edited or recorded using Council's computer networks or resources. Any employee, who becomes connected accidentally to a site that contains sexually explicit or offensive material, must disconnect immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program. The ICT Services Helpdesk must be informed in order that the monitoring software can be amended to include a block to the offending site. The individual reporting the incident will have their details recorded in the incident log.

14. Modification

The Council reserves the right to modify this Policy having given users reasonable notice.

File	Internet Usage Policy	Page	8	Version	Version 1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified