EPPING FOREST DISTRICT COUNCIL

INTERNET ACCEPTABLE USAGE POLICY

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

Version History

Version No	Release Date	Authorised By	Updated By	Approved By	Changes
3.1	April 2006	Adrian Scott / Joe Akerman	Dawn Jolley / Adrian Scott		Version 1.6

Contents

Introduction

Epping Forest District Council's internal computer network is connected to the internet. Everyone with computer access to the internal network has the ability to access the internet, including e-mail and the World Wide Web.

The internet is a resource for the organisation, and it is your responsibility to use this resource responsibly and respectfully. The internet is predominantly for work use, but all employees have the opportunity to use it for personal means in your own time. Personal use should never take priority over work matters.

This policy should make sure all staff and Members (Users):

- Know what they are allowed to do with regard to using the internet during their contracted hours.
- Comply with relevant laws and policies.
- Understand the implications of misusing the internet
- Minimise disruptions to our internet services and activities.

Please also read the Council's E-mail (electronic mail) Policy, which explains the laws relating to e-mail, your rights and confidentiality issues. You must also be familiar with the current version of the Data Protection Policy.

For the purpose of this policy, the term 'user' refers to any individual using Epping Forest District Council facilities.

User Statement

All users granted internet access using Council facilities will be provided with a copy of this statement and general usage guidelines. All internet users must sign the following statement:
"I have received a copy of the Council's Internet Acceptable Usage Policy. I fully understand the terms of this policy and agree to abide by them. I realise that the Council's security software will record, for management use, the internet address (name and other relevant data) of any site that I visit, and may also keep a record of any network activity in which I transmit or receive any kind of data. I acknowledge that any data (messages, files, documents, multimedia content etc) I send or receive may be recorded and stored in an archive file for management use. I know that violation of this policy could lead to disciplinary action which may include dismissal, or even criminal prosecution."

Waiver of Privacy

The Council has the right to monitor any and all aspects of its computer systems, including, but not limited to, monitoring sites users visit on the internet, reviewing material downloaded and/or uploaded by users, and reviewing e-mail sent and received by users. **Users waive any right to privacy, in anything they create, store, send, or receive on any computer or on the Internet.**

This policy will not infringe on any individual's statutory rights.

Amendments

This policy may be amended or revised at any time. Users will be notified of internet/e-mail policies via e-mail on a periodic basis, in addition to continuous posting on the Council's intranet.

Compliance with Applicable Laws and Licenses

Users must comply with all software licensing rules, copyrights, property rights, privacy and all other laws governing intellectual property and on-line activity. All existing Council policies apply to user conduct on the internet, especially (but not exclusively) those dealing with privacy, misuse of Council resources, sexual harassment, information and data security, and confidentiality.

Disclaimer of Liability

The Council will not be responsible for any damages, direct or indirect, arising out of the unauthorised use of its internet resources. Any liability remains with the individual user.

Policy Statement

The Council will seek to ensure the following.

- All Users must use the internet resource in a professional and courteous manner.
- Adequate protections are in place to prevent Users viewing or downloading illegal or inappropriate material.
- Personal use of the internet does not interfere with any work practices.
- Any Users found abusing the internet will have their privilege revoked.
- Heads of Service will ultimately be responsible for ensuring there is no misuse of the internet, software or hardware, by staff in their own service area.
- Users are aware that all sites viewed are logged and can be traced back to the user. Any suspected crime or internet abuse carried out on a Council computer will lead to the Council disclosing this information to the relevant authorities.
- Information on data (messages, files, documents, multimedia content etc) viewed is clearly logged and archived for management use.
- Users must not use the internet resource to offend any colleague or other person, or promote discriminatory behaviour in the workplace.

This policy applies to all Users and all Users must comply with it.

The ICT Service manages the Council's Internet services in accordance with this policy.

The Head of ICT is responsible for developing and maintaining this policy in liaison with the Head of HR.

This policy does not breach your rights under the Human Rights Act, the Regulation of Investigatory Powers Act or the Data Protection Act.

This policy was revised during April/May 2006 and published on xx July 2006.

Guidance

1. At Epping Forest District Council, internet technologies and services are provided primarily for office use, in the direct performance of assigned duties and tasks.

2. Although the internet is generally recognised as a world-wide electronic library of information and services, it is the policy of this Council that all information disseminated through internet services at the Council during work time shall be directly related to the official duties and responsibilities of individuals and organisations fulfilling their assigned work. Likewise, Council Users shall retrieve information from internet services during work time only as it relates to the execution of their **official duties and tasks**.

3. Internet services created and disseminated at the Council are considered official Council computing resources, and therefore are subject to established policies concerning abuse, misuse, or unofficial use by Council Users and contractor employees.

4. It is a disciplinary offence to download or view pornographic material, or anything that can reasonably be considered to be offensive e.g. racist or sexist material or that which demeans any individual or group of individuals.

5. You must not use web content as wallpaper or screensavers. Only use the Microsoft items provided. Any wallpaper or screensaver related text, graphics or movies found to have been downloaded from the internet will be removed.

6. You must not download or install any software from the Internet. This can only be carried out by the ICT Service when appropriate.

7. Our protection system checks where you are going and whether you are allowed to be there. It can deny or allow access, as appropriate. Searching for inappropriate web sites e.g. adult material, drugs may lead to your access being denied.

8. You must never provide to a third party, our corporate postal address, phone number, fax or e-mail address details when surfing the web, unless it is clearly work-related.

9. You must not subscribe to any services, or buy products or services, using our corporate postal address, phone number, fax or email address details, unless it is clearly work-related, defined in your job responsibility and is subjected to the Council's Financial Regulations and Contract Standing Orders. (*Should you purchase personal products or services* ***during your own time****, you are not to provide any Council contact details whatsoever, including those for confirmation responses*).

10. To avoid doubt, Users **may not** use the Council's internet resources for commercial or personal advertisements, solicitations, promotions, destructive programs (i.e. viruses and/or self-replicating code), or any other unauthorised or personal use.

11. To knowingly send, receive, display, print, or otherwise disseminate material that is fraudulent, harassing, illegal, sexually explicit, obscene, intimidating, or defamatory is prohibited. Users encountering such material (inadvertently or otherwise) should report it to management immediately.

12. Unnecessary or unauthorised internet usage 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 usage may also result in negative publicity for the Council and expose it to significant legal liabilities.

General Provisions

Purpose

In support of public services, we encourage the use of the internet to research or share information, improve services and exchange ideas.

Council property

The Council's web-site, links, e-mail address and any account associated with the Council or our services, or assigned to any person, service or function of the Council, is the property of Epping Forest District Council.

Service restrictions

Users must use the internet responsibly and comply with UK laws, Council policies and procedures, and with normal standards of professional and personal courtesy and conduct.

Access to the Internet service is a privilege that may be restricted or removed without notice and without the consent of the user.

Consent and compliance

We will not seek Users' consent before inspecting, monitoring or disclosing Council computer records in their possession. Users must provide access to their record logs if requested.

Misuse

Council policy and legislation prohibit the theft or abuse of computing resources. This applies to internet services and includes, but not limited to:

- unauthorised entry
- use, transfer and tampering with other people's accounts and files
- interfering with other people's work
- interfering with other computing facilities.

Management Reports

All users of the Internet should be aware that management will be receiving relevant reports from the Councils Internet Management System (IMS) to identify potential instances of internet abuse within their service. These reports may be used in investigations and disciplinary procedures.

Specific Provisions

Allowable Use

In general, use of our computer facilities is governed by policies that apply to the use of all Council facilities. We allow personal use of our internet service, subject to the following conditions.

Purpose

Internet services are provided by the ICT service to support our public services and administrative and professional functions.

Users

Only Council employees and Members may use the Council's internet service.

Non – competition

Our internet service is not provided in competition with commercial services to anyone outside the Council.

Personal use

The Council's internet service may be used for incidental personal purposes, provided that it does not:

- interfere with the Council's operation of computing facilities or e-mail services;
- burden the Council with an additional cost
- interfere with the user's employment or other obligations to the Council (**i.e. it should be in your own time**).

Restrictions

Our internet service may not be used for:

- unlawful activities
- commercial purposes which are nothing to do with the Council
- personal financial gain
- Uses that breach other Council policies or guidelines, including policies regarding intellectual property and sexual, racial or other forms of harassment.
- accessing personal e-mail accounts either directly or via the web.

A list of restricted (blocked) site categories is given on page 11

Representation

Internet users must not give the impression that they are representing, giving opinions or making statements on behalf of the Council or any Council services, unless they are authorised to do so. Where appropriate, a disclaimer must be included, such as, 'These statements are my own, not those of Epping Forest District Council.'

False identity

Internet users must not use a false identity.

Interference

The Council's internet service must not be used for any purpose that could reasonably be expected to cause (directly or indirectly) excessive strain on any computing facilities, or unwarranted or unsolicited interference with other people's use of the service.

Security and Confidentiality

1. The confidentiality of communicating on the internet cannot be assured. It may be compromised:

    - by the applicability of law or policy, including this policy;
    - by unintended redistribution; or
    - because of the inadequacy of current technology to protect against unauthorised access.

    Users should, therefore, exercise extreme caution in using the internet to communicate confidential or sensitive information.

2. The 1998 Data Protection Act prohibits people from ‘seeking out, using or disclosing personal information’ without authorisation. Users must take the necessary precautions to protect the confidentiality of all their information, including e-mails.

3. Users should be aware that system support personnel and system administrators sometimes need to observe certain information to make sure the internet service is functioning properly. This is part of their duties and means that they may see the sites you are visiting. They will not:

    - see or read the contents intentionally;
    - view sites for any purpose, other than given in this policy; or
    - disclose or use what they have seen, unless it is in breach of this policy or the law.

    This point does not breach the 1998 Data Protection Act.

4. The Council tries to provide secure and reliable internet services. However, the confidentiality of using the internet cannot be guaranteed.

5. User IDs and passwords maintain individual accountability for internet resource usage. Any User who obtains a password or ID for an internet resource must keep that password **Confidential**. Appropriate care must be taken by individual users to ensure that other individuals cannot access the internet or e-mail facilities using passwords for which they are not authorised. This should involve logging out or locking the PC/terminal if it is to be left unattended. Council policy prohibits the sharing of user IDs or passwords obtained for accessing any network or computer system’s resource.

6. Our computer systems are backed up regularly to protect the systems’ reliability and integrity, and prevent potential loss of data. This data is stored for a period of time and in a location unknown to users. So even though an internet user may have discarded their records, we may be able to retrieve a back up copy.

Archiving and Retention

1. The Council has the capability to maintain Internet archives and retain temporary internet files on the central servers. Each user also has an area reserved for the storage of temporary internet files. These files can be used to trace a user, in the event of any illegal activity found to be taking place on a Council computer.

2. It is not possible to guarantee the longevity of internet records for record-keeping purposes. This is because changing formats and technology may mean older records can no longer be read. Also, without authentication systems, we cannot guarantee that documents have not been altered, intentionally or inadvertently.

3. Internet users should not rely on the system to maintain a lasting record. Sound business practice suggests that information that needs to be kept long-term should be transferred to a more lasting format.

Management and Administration

The Council reserves the right to:

- withdraw Users' access to any computer systems and communication services, including internet services without notice;
- prohibit access to certain internet resources;
- remove or substitute the hardware or software used to access the internet at any time and for any reason without prior notice.

Internet access provided by the Council must be used only for Council business in work time. The Council has software and systems in place that can monitor and record all internet usage. These security systems are capable of recording (for each and every user) each World Wide Web (www) site visit, each chat, newsgroup or e-mail message, and each file transfer into and out of internal networks, and the Council reserves the right to do so at any time. **No User has a right to privacy in respect of his or her internet usage**.

The Council reserves the right to inspect any and all data (messages, files, documents, multimedia content etc) stored in private areas of the network in order to ensure compliance with policy without notice.

If it is found that an account is being used for non-Council related business, Users may be subject to disciplinary action and may in addition be required to pay an appropriate part of the costs incurred.

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

- informal warning;
- denial of internet access for a period;
- denial of internet access permanently;
- disciplinary action, potentially for gross misconduct (i.e. leading to dismissal without any further notice), through the normal disciplinary process;
- provision of information to the police for possible criminal proceedings.

Service Responsibilities and Discretion

Each Head of Service must make sure all internet users have a copy of this policy and must take steps to ensure that the adequate monitoring is undertaken to ensure compliance with it.

'Do's and Don'ts'

Do:

- **Ensure that you understand this policy and in particular the user statement and waiver of privacy permission before accessing the Internet.**
- Comply with Council policies and UK laws that apply to internet usage.
- Use personal and professional courtesy and consideration when using the internet.
- Remember that it is a disciplinary offence to download or view pornographic material, or anything that can reasonably be considered to be offensive – to do so may lead to your dismissal.
- Use protections to deter potential intruders (for example, passwords).
- Take regular breaks from your computer screen, as required by law.
- Remember that all sites viewed are logged and can be traced back to you. We will disclose details of anyone suspected of crime or internet abuse carried out on a Council computer to the relevant authorities.
- Only use the internet for personal purposes in your own time (i.e. before or after work, or during your lunch break).

Don't:

- Breach UK law or Council policy by theft or abuse of facilities and resources.
- Knowingly interfere with other people's use of the internet.
- Knowingly disrupt the Council's internet service.
- Use the internet for unlawful activities, commercial purposes or personal financial gain.
- Use the internet in breach of any Council policy.
- Use the internet to give the impression that you represent the Council, unless you are authorised to.
- Let personal internet use interfere with your work or other obligations to the Council.
- Burden the Council with expenses caused by your personal use of the internet.
- Offend any colleague, or promote/engage in discriminatory behaviour in the workplace.
- Access personal e-mail accounts directly or via the web.

To do so could lead to disciplinary action against you, including dismissal.

Restricted Sites (blocked)

Certain inappropriate Internet sites are blocked centrally by an Internet Management System (IMS) and you will not be able to view them. However, any attempt to view a blocked Internet site is logged to your user ID. New blocked sites are added to the IMS on a regular basis. Requests can be made to the Head of ICT to have a restricted site removed from the blocked list provide the request is support with a sound business case.

The following categories give an example of the websites that are **blocked:**

- **Illegal** – promoting illegal activities such as murder, rape, prostitution, drunk driving, child pornography, paedophilia.
- **Militancy** – militia operations, terrorist activity, war, riots, rebellion, violence, weapons
- **Adult**, including pornography, nudity, sex, strip clubs, erotica, adult humour, homosexuality, bisexuality, sadism, fetishes, masochism
- **Racism**
- Promotion or sales of **alcohol, tobacco or drugs**
- **Alternative journals** – non-mainstream journals, including sex magazines
- **Cult and New Age** – witchcraft, black arts, voodoo, spirituality, UFOs
- **Games and gambling** – sites promoting or allowing on-line gambling or games
- **Hacking** – any sites promoting questionable or illegal use of equipment or software to hack passwords or create viruses
- **Personal / Dating**
- **Web chat**
- **Web Mail**
- **News Groups**

Conclusion

The Internet has become a key mode of communication and is a valuable tool in conducting the Council's business.

However, there are various risks involved and it is essential that good management practices be put in place detailing guidelines on use. This will ensure access is both justified and controlled while remaining compliant with Council policies.

Future Help

If further help in understanding or following these policies is needed, in initially contact the ICT Service desk on extension 4321.