

HARLOW COUNCIL

Information Security Management Policy 2008

Version	Author	Date	Comments
2.0		June 2006	Published version
3.0	Lee French	January 2008	Update and revision. Name changed to include changed date
4.0	Lee French	July 2008	Version number changed and minor revision. Final document
5.0	Lee French	Sept 2008	Revision to password requirement

The Harlow Security Policy

This policy applies to all users of the Harlow District Council network. Users are defined as being full-time and part time employees, home-workers, students, voluntary workers, contractors, 3rd party suppliers and Members. It must be read by all who need access.

Disciplinary action may be taken against any person who accesses or attempts to access Harlow District Council systems without proper authorisation in the form of a valid personal login ID and password.

The **objective** of the security policy is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.

The **purpose** of the policy is to protect the information assets of Harlow District Council from all threats, internal or external, deliberate or accidental.

The policy **ensures**:-

Confidentiality of information will be assured

Integrity of information will be maintained

Information and services are available to authorised users when required

Regulatory and legislative requirements will be met

Information security training will be available to staff

All breaches of the security policy, actual or suspected, will be logged, reported and investigated, and could result in disciplinary action being taken. Continuity plans exist to support the policy.

Each line manager is responsible for the implementation of the policy within their own business areas and for adherence by their staff.

It is the responsibility of each Elected Member, member of staff, voluntary workers, students, contractors and third party suppliers using the Council's ICT network to adhere to the security policy; the line management arrangements described within it apply to members of staff only.

This policy has been developed with regard to:-

- The British Standard on Information Security Management (BS7799/1S017799)
- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The Copyright, Design and Patents Act 1988
- The Freedom of Information Act 2000.

All officers and members are also referred to the Corporate email policy, and the relevant Council guidance which governs officer and member conduct.. These must be read in conjunction with the ICT Security policy.

The Senior ICT Manager (or equivalent authority) is responsible for maintaining and providing advice and guidance on implementation of the security policy. The policy has been developed to be consistent with Data Protection and Freedom of Information requirements, and will be published on the Intranet.

Summary of Key Guidelines	5
Physical Security.....	5
Using your workstation.....	5
Protecting your Information	5
Back up and Recovery	6
System development.....	6
Background	7
Introduction	7
The need for Information Security	7
Statement of Intent.....	7
Definition of a breach of information security	8
Responsibility.....	8
Reporting Suspected Incidents	8
Using Workstations.....	9
Acquisition and Use of Computers	9
Ownership of Software.....	9
Copying of Software.....	9
Physical Security.....	9
Securing the Physical Location of the Workstation	10
Ensuring Business Continuity	10
Back up and Recovery	10
Moving Computer Equipment.....	11
Environmental Considerations	11
Protecting Access to Information	11
Disposal of Information	11
Passwords	11
Using Portable Devices.....	12
Accessing the Internet	12
Internet Usage	12
Introduction	12
Obtaining Internet Access	13
Web Awareness.....	13
Misuse of the Internet.....	13
Web Site restrictions	14
Internet monitoring and Reporting.....	14
Email.....	15
Email Protocol.....	15
Do you need to send an email?	15
Copying for Information.....	16
Time Management	16
Global emails	16
Unsolicited mail.....	16
Attachments	16
Out of Office.....	16
Mail Boxes	17
Working at home or other remote locations	17
Homeworking	17

Access from home	18
Server Security	18
Location	18
System Access	18
Application, File and Print Servers	18
Viruses and Spam	19
What is a computer virus?	19
Reporting a virus.	19
What is spam?	20
Reporting faults	20
Equipment faults	20
Theft or damage.....	20
Acquisition and Disposal.....	21
Obtaining and Maintaining Equipment	21
Disposal of Obsolete/Redundant Equipment	21
Disposal of confidential waste	22
Other Issues	22
Starters and Leavers.....	22
Housekeeping	22
Developing your own systems	23

Summary of Key Guidelines

Physical Security

Don't leave your workstation active when not in use. Always use a password-protected screen saver or log-out completely.

Think about the location of workstations to avoid unauthorised viewing of your screen, or to reduce the chance of theft. Obtain advice where necessary from the ICT Service Desk.

In areas where equipment is particularly vulnerable, consider physical methods to secure it, such as security cages, chains or desk-locks.

Do not move computer equipment yourself. Instead, contact the ICT Service desk who will arrange to have it moved. Equipment must not be relocated other than by ICT staff for the purposes of network management, insurance and audit.

Managers must have written procedures available to support any action that needs to be taken to access the data in the event of a problem.

Using your workstation

Always abide by the requirements of the Data Protection Act

Your workstation should normally be used for authorised Council business although occasional personal use is permitted if agreed by your line manager and during designated breaks from work. Access to some activities and websites will always be prohibited.

When you visit an internet site you will leave traces of your visit in a number of places. Your use of the internet is monitored. A series of internet monitoring reports are produced and, as appropriate, passed to line managers. These reports include analysis of corporate, departmental and individual use.

The Systems Administrator is also able to monitor e-mail communications but this will occur only in exceptional circumstances, such as when the employer has reasonable grounds to consider serious misuse is taking place. Improper use of e-mail may lead to Disciplinary proceedings.

Only use approved software obtained through IT and installed by authorised staff

Do not make illegal copies of software. The council can be subject to large fines for using illegal software, and you may be disciplined.

Be on the look-out for viruses, especially if you use a PC, and report all occurrences to the ICT Service Desk

All machines attached to the Council's Network have anti virus software installed. For assistance contact the ICT Service Desk.

Protecting your Information

Ensure that a policy has been agreed in your Section concerning sensitive information, and then protect it as appropriate.

Remember that data copied to external devices (CD, DVD, Memory sticks etc) is especially vulnerable. Always password protect this data and consider encryption if the data contains personal information. If unsure, contact ICT who will be able to advise and assist if help is needed.

All workstation users are allocated a unique log-on ID, and are asked to choose a password. This must be at least seven characters long and contain at least one capital letter and one number. Never share your log-on ID

or disclose your password to others. Choose a password that you will be able to remember, but is not easy for others to guess.

If someone else needs access to data that you maintain, ensure that it is stored in an area available to those persons that need access on a shared network folder, or if appropriate store the data in the Electronic Document and Records Management System (Meridio). For advice contact the ICT Service Desk.

If you forget your password or you are denied access to the Council's network, you must ask the ICT Service Desk for your password to be reset.

Consider applying extra security where appropriate for your section.

Delete sensitive data by overwriting where possible

Be especially careful if you travel with a laptop, or work from home.

Retain or destroy records as agreed by your Section's security and document policy, for advice you can contact the Information Security Officer (to be designated).

Back up and Recovery

If you hold any applications or data on your local drives (i.e. the disks physically located in your desktop computer), remember that you must back these up regularly or run the risk of losing this information. PC disk drives can and do fail periodically, and unless you have a workable backup with which to rebuild your PC, all the information will be lost.

To ensure they are workable, these backups must be stored securely and tested regularly

It is much less risky to store all data on networked drives on the corporate network, as these are backed up daily.

As always, if in any doubt, contact the ICT Service desk

System development

Have any locally developed spreadsheets or other applications checked independently to ensure that there are no errors, which could force you unwittingly to use erroneous information.

Use of Microsoft Access as a development tool should be carefully considered. It should not be used to develop applications or databases which are critical to the business, likely to be used long term, or which need to be networked.

No development in Microsoft Access should be undertaken without appropriate training in both the product and the Harlow District Council development standards, and where necessary, reference to change control procedures.

Applications and data sets that have been developed will need to be registered with the ICT Development team to ensure they are secure, and to ensure the Council's conformance with both the Data Protection Act and the Freedom of Information Act..

In many cases it may be appropriate to develop systems using a more appropriate, corporate tool, such as SQLServer .For advice and guidance on developing applications contact the ICT Service Desk. For information on corporate ICT training provision contact Human Resources.

Background

Introduction

Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and ensure service delivery.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it must always be adequately protected. Harlow District Council places heavy reliance on the use of computers and computer systems, to support its services. It is therefore important that these facilities are used in a secure, efficient and legitimate manner.

Information security has the three key components - confidentiality, integrity and availability.

Confidentiality relates to the protection of sensitive information from unauthorised disclosure,

Integrity refers to safeguarding the accuracy and completeness of information and computer software, and

Availability is concerned with ensuring that information and vital services are available to authorised users when required.

In order to promote information security within the authority this document forms the basis for the Council's Information security policy. In preparing this policy the provisions of the British Standard on Information Security Management (BS7799), the international standard for IT Service Management (ISO20000), and industry best practice based on the IT Infrastructure Library standards, have all been taken into account. The guidelines contained in this policy are aimed at achieving a minimum level of security. In certain circumstances a higher level may be appropriate.

The need for Information Security

Increasingly the Council, its information systems and networks are faced with security threats from a wide range of sources. These include, computer assisted fraud, viruses, hacking, use of illegal software, loss or theft of data, and inappropriate use of e-mail and the Internet.

To establish an effective level of Information security it needs participation by all, whether employees, councillors, or partners, in order that services are both protected and available when required.

Statement of Intent

The Council is committed to using information technology and computer systems in a secure, efficient and legitimate manner. It fully supports the objectives of legislation relating to the use of computers and is committed to preventing the unlawful use of computers and data. The Council's policies on Data Protection and Freedom of Information deal with these two aspects in detail.

It is the ultimate responsibility of each manager or Elected Member to ensure that the computer processes and practices within their service/area of responsibility are in accordance with this policy. The policy will be kept updated by the Senior ICT Manager (or equivalent authority) as required by the Policy and Resources Committee.

Every individual has a responsibility for information security. The Council will take action as appropriate, including disciplinary action against individuals, in the event the security policy is breached

Definition of a breach of information security

A breach of security is defined as a failure to comply with recognised standards of work relating to the use of computers, or the confidentiality of data as defined in this Policy. It also covers situations where an unauthorised person has accessed, or is suspected of accessing Council data or software without permission.

Signs that security has been breached include:-

- An unauthorised person is seen accessing computer information
- You believe that somebody else has obtained your log in details and password
- You see that data has been changed in an unexpected way
- Data copied to external devices has gone missing
- Confidential information is found in the public domain
- A computer is found logged in when it had previously been disconnected
- Documents have been accessed from your computer whilst it was left unattended.

Responsibility

Every member of staff and elected member is responsible for safeguarding the information that is vital to the working of Harlow District Council. Directors, Heads of Service, managers and supervisory staff must ensure that their staff complies with this policy

The Senior ICT Manager is responsible for ensuring that the access privileges to user accounts is maintained on a 'need to know' basis and is regularly reviewed.

Users must keep all confidential data secure

Users must ensure that their passwords are kept secure and not shared for any reason.

No software other than that legally acquired by or on behalf of the Council shall be loaded or used on the Council's equipment. The unauthorised copying of software is not permitted. Software/hardware owned by the Council should not be used for personal work without prior line management agreement.

Computer equipment must not be removed from site without permission.

Games, other than those supplied as standard, must not be loaded or played on any computer owned by Harlow District Council.

Networked file servers must be used for data storage and for backups.

Use of personal information, contrary to the provisions of the Data Protection Act 1998 is not permitted.

The configuration of the equipment must not be altered without permission and supervision.

The Computer Misuse Act 1990 also prohibits:-

Unauthorized access to computer material.

Unauthorized access with intent to commit or facilitate commission of further offences.

Unauthorized modification of computer material.

The above list covers the key breaches but is not intended to be exhaustive.

Reporting Suspected Incidents

Any violations, observed or suspected, of this security policy must be reported to your line manager or to the Senior ICT Manager (or equivalent authority).

Using Workstations

Acquisition and Use of Computers

Strict procedures for the acquisition of computers, software and all ICT related equipment are laid down by the Council, and all such purchases must be handled through ICT, who will advise you on the equipment you need, give or help you to obtain the necessary authorisation, and assist with all aspects of the procurement process. It must be noted that unauthorised equipment will not be connected to the Council's network or supported and maintained by ICT support staff.

Ownership of Software

Software or data files developed by employees on Harlow District Council equipment remains the property of the Council and can only be offered for use outside the Council with management approval and appropriate safeguards. IPR (Intellectual Property Rights) for all software or data files developed as part of normal duties, using Council equipment or facilities, or during normal work hours, remains with the Council

Copying of Software

Software (including manuals etc.), which has been bought or purchased from a third party, is normally covered by strict licensing rules, which generally mean that the software cannot be copied or installed onto more than one PC. Even software, which is installed onto a network file-server, is normally limited to a set number of users. If you are unsure as to the position on a particular item of software, you should contact the Service Desk. On no account should any employee of the Council make illegal copies of software, data or documentation.

Software must always be obtained through the proper channels. Any alternative - including the loading of "free" software from outside the organisation - brings, as well as the likelihood of a breach of copyright laws, a risk of contamination by viruses.

The ICT Service Desk should be informed of any third party software that is to be installed on Council equipment so the Corporate Asset Licensing Inventory can be kept up to date. A copy of the license should also be sent to the ICT Service Desk for central storage. Periodic audits of equipment are undertaken, and any software found for which appropriate licences cannot be confirmed will be immediately removed.

Physical Security

You should never leave a workstation unattended and logged on. If you leave it in a state where others can access information, then any inappropriate use will be tracked to your log-on ID, and you will be held responsible. Remember also that if you use electronic mail, leaving your computer unattended could allow others to send email or visit web-sites in your name.

There are two ways to protect your screen from unwanted access:

- Whenever you leave your workstation unattended, log off the system. This should certainly be the case if you go away from your computer for a lengthy period, such as during the lunch hour.
- Use Settings/Windows Security to lock your workstation. Putting in your Windows password will unlock your workstation.

Your manager should decide on a policy according to the level of sensitivity of the information held by your section.

Securing the Physical Location of the Workstation

If the information accessed from your computer is particularly sensitive, then the workstation itself should be located in an area where there are physical security or access controls. Even the positioning of the screen can be important: sensitive information should not be easily visible to those unauthorised to access that information, be it public or staff. Careful consideration should be given before positioning workstations on reception desks or facing windows that are adjacent to public foot paths.

The storage of data on local or portable drives is strongly discouraged. Appropriate security can be accommodated on network drives. Contact the ICT Service Desk for advice

Computers, disks and tapes can easily be damaged or stolen; there are incidences of crime where computer chips and hard disks are stolen rather than the whole computer, and the security of your location should be subject to particular consideration. If your computer is in a particularly vulnerable location, additional physical security can be used, such as locking devices which secure equipment to fixed surfaces. Advice on this can be obtained from the ICT Service Desk

Ensuring Business Continuity

The ability of the business to function efficiently can be hampered by the loss of systems and/or data, either temporarily or permanently, and to minimise this risk, contingency plans must be employed. The Council has a corporate disaster recovery plan which will protect the information held on the corporate server network, but this will not cover applications or data held on individual PCs. Your section should have clearly documented contingency plans to enable recovery from any disaster involving computerised systems or information held locally to you.

ICT Services will be able to help with the temporary provision of alternative computers, etc., but you should have full documentation of all systems in use on workstations, particularly those which have been developed by staff in the Section. Remember that it will be equally disastrous for your operation if the only member of staff who knows about a particular system becomes temporarily or permanently unavailable for any reason.

Back up and Recovery

For PC users it is essential to ensure that all files which are crucial to the working of your business, are held on a network drive on a server, and not retained and filed on the local c: drive. It is essential from both a security and recovery point of view that all such files are saved to a network drive. Data stored on the Corporate Network, including all Citrix servers, is secured daily, whilst data on your local hard drive is not automatically backed up and could be lost if your PC fails.

It should be noted that the ICT service cannot guarantee the security and availability of data which is stored on local drives.

Storing any important data only on your local drive is therefore actively discouraged, but where this is deemed necessary, local security arrangements must be in place to back up this data, and you must test the back-ups work by restoring data on a regular basis. For advice on local security issues contact the ICT Service Desk.

Store back-ups securely, both on and off site. Ensure that written procedures are in place to clarify the action required should it be necessary to restore the data.

Corporately taken backups are removed off-site for safe and secure storage in line with the Disaster Recovery Strategy.

If your workstation is vital for provision of your service, agree contingency plans in your Section to be used in case of disaster or disruption. If you are unsure and need advice contact the ICT Service Desk.

Moving Computer Equipment

Equipment must not be relocated other than by ICT staff. This is to protect the equipment itself, to ensure continuity of service where connection to other equipment is involved and to comply with Health and Safety Regulations. Contact the ICT Service Desk to have equipment relocated.

Movement of IT equipment should also be recorded on the inventory records, particularly as this may otherwise adversely affect insurance cover if not properly maintained.

Environmental Considerations

Computer equipment can be damaged by heat, direct sunlight, dust, smoke, spills of liquid, static electricity and so on. Care must be taken therefore when sitting at computer equipment, with attention also being paid to the requirements of Health & Safety regulations. It is the responsibility of local Management to ensure workstation assessments are carried out.

Do **not** attempt to dismantle computer equipment for any reason.

Protecting Access to Information

Common sense will normally indicate the level of sensitivity of information you deal with. However, additional security measures are available such as assigning passwords to files and encryption. Encryption should always be considered when copying data containing personal information to an external device of any kind (CD/DVD, laptop, Memory stick etc)

Advice on protecting software and data can be obtained from the ICT Service Desk.

Disposal of Information

It is important to dispose of information, which is no longer needed according to the level of sensitivity, particularly in the case of personal information covered by the Data Protection Act. The shredding of documents may be appropriate in many circumstances, and you should remember to destroy fully the same information held on computer disk, this will include the emptying of "recycle bins" where appropriate.

Passwords

The password is a key to information and as such should be guarded carefully. It provides access to your account on the network, which is used to track activity and, therefore, is similar to your PIN number on Bank cards.

Only the ICT department has the ability to overrule passwords, and thus gain access to your information. This is only ever done in exceptional circumstances, for example if an individual is on long term sick leave or is unavailable for an extended period, and will always be recorded. It may also be done at the request of a Head of Service in cases of suspected misconduct.

Any password must be at least seven characters long, and contain at least one capital letter and one number to make it harder to guess. The more sensitive the information, the more complex the password should be - but not so complex that you cannot remember it! In order to access the Council network, you will be forced to periodically change your password (currently every sixty days) and you will also be forced to use a different password to the last ten you have used, to prevent the same passwords being used constantly.

Many of the applications used by the Council for specific services (i.e. Housing's Orchard system) contain an additional level of security, and will also require a password in order to gain access. The requirements for individual applications may differ from those for corporate network, and the local system administrator will inform you of the requirements for these specialist applications.

Do not use obvious passwords, such as your name, the name of your spouse/children/dog, the make of your car, etc.

Do not necessarily wait for the system to prompt you to change your password. Change it regularly - once a month, for instance.

Avoid writing your password down at all, and certainly do not do so where it can be easily found. Do not lend your password for others to use - and do not ask or let others tell you their password. If you do not have access to something on the computer, either you should not be accessing it or you should ask for permission to be granted and to be set up as a user of that system.

If you forget your password you will need to authorise its release via the ICT Service Desk or appropriate systems administrator, where the request will be logged and the password reset. You should immediately reset the password to something known only to you.

Don't assume however, that failure to access the network is related to your password, there are other technical problems which may cause this difficulty. You should log a call with the ICT Service Desk.

Using Portable Devices

A portable device could be a laptop, hand held, palm top, a mobile phone, memory stick, or DVD/CD - in effect any device or medium that can hold personal information. Where possible, implement power-on password protection for your portable device. Be especially careful if you use your portable device in an unsecured location. Lock away your portable device and any disks or portable storage devices when not in use.

Never leave the portable device in a car overnight, or even worse, in open view.

If you have access from a remote location to a computer system at the Council, you may expect to encounter strict access security measures designed to prevent outsiders from "hacking" in to the system.

If you use a portable device which holds personal information, then serious consideration should be given to using encryption to protect the data in the event of the equipment being lost or stolen.

If you need to copy personal information to an external medium, ensure its whereabouts is known at all times. . Never send unencrypted personal information to any third party by an unsecure method (i.e. via the public postal service).

Accessing the Internet

Internet Usage

This policy applies to all users of the Harlow District Council network as defined in section 1. This section must be read by all who need access to the Internet via the Council network.

The Council has a dedicated connection to the Internet which is protected by fire-walls and filtering software to protect the Council's network from attack from external sources, to protect the unwary from unwanted or inappropriate material, and to prevent users of the Internet service abusing the facility..

The service is made available to all Elected Members and all staff after approval is received from their Line Manager or appropriate authority. All access is monitored for appropriate use and tracked against your own log-on ID. It is essential, therefore, that you only access the Internet using an account set up specifically for you.

Introduction

Threats from the Internet pose increasing risks to computer installations and networks regardless of size or location. Harlow Council is not exempt from these threats. Some examples include; virus attacks, which can

corrupt data or degrade services, Internet worms which can undermine security, or Denial of Service attacks which flood systems with bogus requests for data, preventing legitimate users from using a service. In response to these threats we have implemented a number of security measures including:

- Educating staff to the pitfalls of the Internet and the consequences of misuse.
- Limiting staff access to the Internet on a 'need to have' basis.
- Regulating access to inappropriate web sites.
- Monitoring Internet use and reporting suspected misuse.
- Scanning web traffic, servers and PCs for viruses, Trojans or other malicious code.
- Limiting use of file transfer facilities e.g. FTP.
- Restricting external access to the Council's network using firewall technology.

Obtaining Internet Access

The Council provides the Internet facility for business use, although occasional personal use is permitted if agreed by your line manager. Monitoring of usage is a local management issue, and it is the responsibility of each manager to ensure that conditions of use are being adhered to. It should be noted that the provisions of this document apply equally to both business and personal use of the Council internet facility.

Personal use is forbidden during your contracted hours of employment, other than during designated breaks.

If approved, your Line Manager will submit a request for internet access to the Service Desk, who will set-up your Internet account.

Web Awareness

Your use of the internet is monitored. It is important to note that when you visit an internet site you leave traces of your visit in a number of places. These include:

- The web sites you visit.
- The web monitoring software used by the Council to manage internet access.
- Your history file on your internet browser.
- Your 'cookies' file in your PC or Citrix profile.

Cookies are placed on your PC when you visit some web sites. The cookies allow the sites to build a profile of you as a customer and can be used to send you special offers etc. specific to your customer profile.

We strongly advise against use of web banking (or similar applications) from workstations supplied for use by council employees or members. These applications store personal information e.g. bank account details. The Council will not be held liable for any financial losses that occur as a result of using web based banking facilities on its network

Misuse of the Internet

Remember Internet access is provided primarily as a business tool and should not be misused. Misuse will be considered to be a breach of this security policy.

Examples of misuse include, but are not confined to:-

- Any use prohibited by corporate policy.
- Use for personal business or activity intended to achieve personal financial gain.

- Making confidential information available to unauthorised individuals outside Harlow Council.
- Sending, forwarding, browsing, exporting from or importing any materials that are or could be in any matter whatsoever, considered to be pornographic, obscene, offensive (whether from a sexual, racial, political, religious or any other perspective), defamatory or of a criminal or subversive nature.
- Inappropriate services (as specified in web-site restrictions).
- Downloading and installation of application or executable software without prior approval of ICT Services. Approval can be sought by contacting the Service Desk.
- Any use that could bring Harlow Council or its employees into disrepute.

Web Site restrictions

Internet access at HDC is for providing access to sites relevant to Council business. In line with this, web access is not provided to sites that can be categorised as follows:

Adult or explicit	Chat	Criminal skills	Weapons
Drug alcohol or tobacco	Gambling	Games	
Glamour/intimate apparel	Hacking	Hate speech	
Personals & dating	Usenet	Violence	
* Web-based mail e.g. hotmail	Video sharing e.g. YouTube	Social networking e.g. facebook, MySpace	

* It is possible that access to Web-based mail may be permitted, although this will normally be restricted to outside of core working hours.

If you accidentally gain access a site that falls into one of the categories above please contact the Service Desk immediately and provide them with the site details.

This action has 2 benefits:

- It allows us to block this site, preventing other users from accessing it inadvertently
- It highlights to ICT Services that you did not intend to access the site.

It should be noted however, that if you fail to contact the Service Desk, or repeatedly visit the inappropriate site, this will be classified as misuse.

Some users will have valid requirements to visit a web site, or category of sites, where access is not normally available. In such cases, details of the requirement should be passed to your line Manager, who can arrange access via the Service Desk.

Internet monitoring and Reporting

A number of tools are available within ICT to monitor and report on internet usage. These are used to support the local management of internet access, and prevent internet misuse.

For example, the Council uses specialised internet monitoring software on its web servers, which regularly monitor usage. A series of Internet monitoring reports are produced and appropriate ones are passed to line management. These reports include analysis of Corporate, Departmental and individual use.

Email

Email Protocol

A separate corporate policy on email is published and available on Infonet. It can be found under Customer Services ICT key documents, and all users of email should familiarise themselves with the content of this document. The following should be read in conjunction with the email policy.

E-mail is a powerful, useful tool that assists the Council to provide services in a more efficient manner. Its prime use is therefore for Council business.

Individual user accounts are created by I.T. Services, upon receipt of authorisation from line managers. Accounts and passwords are set up and it is the responsibility of the individual to ensure that their password is kept safe - the individual is responsible for all messages sent from their address.

Courses can be arranged for new employees to learn about the Council's system. Please complete the Training Needs Form and send to HR. Courses will be provided when sufficient numbers require training.

E-mails that go outside the Council must have the standard disclaimer attached.

Use of e-mail for private messages is permissible, provided it does not take priority over Council business. It may not be used for political or commercial purposes.

[Members may publish their Harlow Council e-mail address in a way that is merely incidental to the nature of any leaflet or publication and is clearly intended simply to facilitate easy contact with residents etc in the area. Notwithstanding this advice there might be situations where an attempt to utilise a specific Member's address for a general party purpose might constitute misuse of the Council's resources. Equally highlighting or drawing undue attention to the address in a manner designed to draw attention to a Member's status in an otherwise non-political role might also breach the Code of Conduct.](#)

E-mail usage is subject to Council policies on Equal Opportunities, Harassment etc, and officers and members should also ensure they are familiar with and comply with the relevant Council codes of conduct as it applies to use of email.

In common with other data, ownership of emails contained within email accounts on the council systems remains with the Council and not the individual.

In exceptional circumstances, it may be necessary to gain access to an individual's email account in order to ensure the Council can continue to fulfil its role. For instance, when an individual is off sick or otherwise absent for a protracted period, and cannot be contacted, or where no provision has been made to forward emails appropriately during an extended period of absence. In these circumstances, the Head of Service of the account holder concerned, or the Chief Executive in the case of member's email accounts, can request the Senior ICT Manager to provide restricted access to an individual's emails.

Mail may be monitored by the Systems Administrator, although this will occur only when the employer has reasonable grounds to consider serious misuse is taking place. Improper use of e-mail may lead to Disciplinary proceedings.

The following is a general guide to good practise in the use of email:

Do you need to send an email?

If you are likely to be shuttling emails about the same subject back and forth it might be better to call the person or arrange a meeting. Emails should not be a substitute for face to face communication where that is a better way of working.

Similarly, consider carefully whether to assign a priority to an e-mail, High Importance Flags must only be assigned to messages that require immediate attention, messages with a more social content should be flagged as of Low Importance.

Copying for Information

There is a tendency to copy people into emails for information. This can give the impression, where it is desired, that you have let people know about something. It can be a way of covering your back on difficult issues. But there is no guarantee that the recipients have either read or understood the issue. And it simply adds to their inbox. Do so only with care.

Time Management

Like ringing phones emails can eat into valuable work time and diminish the service we are able to offer our customers. They eat up real time. Before you use email, consider whether it is the best use of your and our customers' time.

Global emails

Facilities exist to send global emails - those sent to all email users on the system - but this is not to be used by individuals. If there is a need to send a global email, it must be drafted, approved by your head of Service, and then sent to the Corporate Governance Section for distribution. ICT have the facility to send global emails only to give urgent warnings of unplanned service interruptions...

If you wish to communicate with all those on the Council email list, if, for instance, you are seeking new equipment or selling something, use the Market Place on Infonet. For instructions for this click on the Market Place button.

Unsolicited mail

If you receive mail from an outside source, directly to your Harlow.gov address, it will have been virus checked. Nevertheless you should take care in opening it. If in doubt - delete it.

Delete junk mail immediately.

If you receive messages warning of viruses, please forward them to the IT Service Desk immediately, and delete them from your mail box.

Attachments

Please don't use email to circulate attachments internally - it is better to publish the material on infonet, or store it on a network drive, and then mail those who may be interested in it, to tell them where it is.

If you are sending large attachments outside the Council compress them first using Zip.

Not everybody has access to all software, so if your attachment is not Word or Excel, the recipient may not be able to read it.

When receiving attachments, consider whether you need to store them in your mail folder.

Out of Office

When you are away from the office, use the Out of office Assistant to let correspondents know. If you are likely to be away for some time, assign read access rights to your mail to another person in your department, who can deal with urgent correspondence on your behalf.

Mail Boxes

Mail box size limits are generally set at 100MB, which is considered to be more than adequate if email is being actively managed. The system will generate warnings when the mail box size reaches 80% capacity. At 90% mail can no longer be sent, and at 100% no further email can be received. Archive or delete mail to reduce the volume in the mail box.

Deleting mail moves it into the Deleted Items folder - to make the space available delete the contents of this folder regularly. You can set a default to delete Deleted Items on logging out if you wish.

If you file a message with an attachment, the attachment is also stored in the mail folder. If the attachment is large it is better stored on your H drive (right click the attachment, click Save As and save in an appropriate folder), then press the delete key and the attachment is deleted.

Organise your mail box by creating suitable folders to hold mail items.

Instructions on how to manage your mail box are contained in the corporate email policy, and there are some tips available on the IT Infonet pages.

Working at home or other remote locations

This policy applies equally to Council work done at home or other remote locations, whether on Council equipment or on your home PC. Indeed, the surroundings are less well controlled than in the office, and extra care must be taken to maintain confidentiality and protect the information.

Homeworking

The Council has a homeworking policy whereby officers are able to work from home using electronic communications to access council IT systems.

Homeworking is at the discretion of the relevant Service Manager and subject to conditions set by the Council's Human Resources Service including a satisfactory home assessment undertaken by the Council's Health & Safety Officer.

Access to Council IT services will be achieved using a broadband Virtual Private Network (VPN) connection. This is provided by means of a remote access facility available via Harlow's website which can be set up on request to the I.T. Service Desk.

Where necessary, IT Services will provide the IT equipment necessary to meet the needs of each individual homeworker. Where this equipment comprises a Personal Computer (PC), it will be password protected.

Equipment provided by the Council under this scheme should only be used in connection with council business, and will Remain the property of the council at all times.

The cost of any equipment provided, and cost of providing and rental of any broadband internet connection will be charged to the relevant department Service manager.

IT Services are not generally able to provide home visits for support and maintenance, but will endeavour to do so whenever possible. Those who use Council equipment at home must be prepared if necessary to return the equipment to the Council ICT Department for repair and/or inspection.

The Homeworking scheme may be withdrawn at the Council's discretion, at which time all equipment must be returned to the Council both in good working order and in a timely manner. The broadband line rental will be either terminated or transferred to the individual as preferred.

Access from home

The Council has an 'Access from Home' policy whereby office based staff are able to access Council IT systems from home. This is aimed primarily at those officers who have support responsibilities or require to access systems on an occasional basis.

It is assumed that Officers wishing to use this service will normally use their own IT equipment and broadband internet connection. Access to the Council network will only be permitted via the Council's remote access facility. This can be set up on request to the I.T. Service Desk.

Access from Home is at the discretion of the relevant Service Manager

Server Security

Location

File servers must be housed in secure locations. Invariably, this will be in the computer suite in the Civic Centre. Here they are in a clean, air conditioned environment, with UPS (backup power supplies) available. System security is easier to manage, and off site storage of data is also provided.

The computer suite has its own access control system and access is restricted to authorised staff only.

Very occasionally, however, servers may be located elsewhere in the Council and all aspects of physical security must be employed to safeguard them. Extra care must be taken to ensure the environment is free from excessive dust, and that air conditioning is available where the heat generated by the servers requires it.

Networked servers should only be installed in conjunction with the ICT department who will determine the most suitable location.

System Access

Administrator and root passwords - this type of system password should only be used in an emergency. It should not be the default operator log on account. Although tasks will need to be carried out on the server with Administration or root privileges, specific user accounts can still be given the correct level of access. This then allows an audit trail to be built up for each user.

ICT will hold all high level administrator and root passwords for all servers. These will be kept sealed and securely stored within the ICT offices so that they are available should they be needed in an emergency. They will usually only be used to set up the initial high level user specific accounts.

Application, File and Print Servers

The network involves the use of central computing resources which allows for the sharing of computer applications, files and printing facilities. These are maintained and managed. The file-servers are:

- Protected from unauthorised access by passwords, etc.
- Located in a secure environment to ensure only authorised personnel may gain access to their physical environment.
- Maintained and managed by ICT Services, including back-ups and capacity planning.
- Equipped with appropriate software and managed by appropriate procedures to prevent virus infection.
- Have the number of people who can access it strictly limited according to need, with those people given access only to those parts of the system required by their function.
- Monitored to ensure access rights are used appropriately and security violations are tracked and followed through to a successful conclusion.
- Included in the corporate disaster recovery planning
- Managed by appropriate procedures and software tools to ensure availability levels are maintained
- Replicated to allow for system development and testing

Viruses and Spam

What is a computer virus?

A computer virus is a type of computer program written with varying levels of malicious intention which spreads itself from computer to computer by automatically attaching itself to files transferred by floppy disk, email or direct connection, including modem links and USB drives. If a virus infects a network, then it can affect the computers of everyone attached to that network.

The damage that viruses can do varies depending on the intent of the virus author. Some provide merely a nuisance, such as the writing of unexpected screen messages, whilst others are designed to destroy all the information on a hard disk. Some viruses are very subtle in operation, quietly altering files in some small way, which is not immediately apparent, but which compromises the accuracy of the data you are using. At the very least, a virus that replicates itself consumes resources and can eventually bring your computer to a halt.

The Council has implemented a number of measures to try to secure the network from the infection from viruses. Each PC connected to the network has an antivirus product running in the background which monitors file activity and detects any infection. As a secondary measure, an alternative antivirus package is installed to monitor file activity on the file servers, alert the systems administrator should it detect an infection, and enable it to be dealt with in the appropriate manner.

In addition, any e-mail which is sent into the Council via the internet is monitored by another antivirus package and when any infected files are detected, they are moved to a safe area of the system and a message sent to the sender, recipient and systems administrator to inform them of the infection.

Reporting a virus.

Despite all this protection, it is not possible to be certain of avoiding viruses. If you suspect that anything is amiss contact the ICT Service Desk immediately. **Do not try to remedy the situation yourself.**

Signs of possible virus activity include:

- Your computer slows down unaccountably.
- You begin to run out of computer memory.
- Programs or files increase in size or change name.

- Unexplained errors occur, particularly showing a pattern.
- Strange messages or effects appear on your screen.

It is a disciplinary offence to deliberately introduce a virus.

What is spam?

Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages, with the most widely recognised form of this being [e-mail spam](#). Spammers are numerous, and the volume of unsolicited mail has become very high – estimated currently at over 80% of all email traffic. The results of this activity include lost productivity, degeneration of email systems, fraud, and increasingly the spread of viruses and other threats.

Spamming should not be confused with legitimate, targeted advertising, product offers, invitations and so forth which you would expect to receive as part of your work or interests.

As with viruses, the Council employs several countermeasures to prevent spam mail from getting onto our system, with the vast majority of it trapped by intervening software. But occasionally, this filter will not be able to differentiate between real email and spam. When this happens it will quarantine the message and ask the recipient to decide whether or not it should be released.

Even more occasionally, a spam message will get through. If this occurs, please do not respond to it, but forward it to the ICT Help desk so that steps can be taken to prevent a recurrence.

Signs of spam include:

- Emails from sources you do not recognise, offering products or services in which you have no interest.
- Emails which ask you for personal information (particularly those purporting to originate from banks asking for account details or pin numbers)

Reporting faults

Equipment faults

If you experience any hardware or software fault, and there is no obvious answer which can be obtained from a colleague in your office, then you should ring the ICT Service Desk. Your call will be resolved by the ICT Service Desk or logged and passed to the appropriate person to deal with. You should always be given a call reference number.

When reporting problems or faults please remember to supply the ICT Services Desk staff with the following:-

- Your name
- Your location
- Your contact number
- The asset number of the equipment (if known).

Theft or damage

Material damage.

Computer equipment is insured as part of the Council's Insurance policy, providing it is included in the appropriate equipment schedule.

Data and information

Part of the cost of loss may be the restoration of data files and software. As stated before, storing these on network drives will minimise this risk.

However you should be aware that insurance will not necessarily cover the cost of materials, labour and computer time expended in reproducing systems and this may be recharged.

Additional expenditure

This covers additional expenditure reasonably incurred if use of computer equipment is interrupted or interfered with as a result of any of the insured risks. These include fire; lightning; explosion; theft; riot and civil commotion; accidental damage; storm and flood etc.

Procedures for notification of new equipment

The insurance inventory is annually updated from the main inventory held in Central ICT. This can now record insured items irrespective of whether it is maintained by a third party or centrally.

The Council's insurers only require certified inventory information once a year, prior to the policy renewal date of 1 April. All services are responsible for ensuring the asset inventory is up to date and accurate.

Acquisition and Disposal

Obtaining and Maintaining Equipment

All computer equipment purchasing is carried out by ICT Services, initiated by a call logged with the ICT Service Desk. A standard business case form must then be completed, before the equipment can be ordered and installed.

Computer equipment is purchased subject only to the requirements of Standing Orders, EU Directives and must comply with Harlow District Council's Corporate Standards for Procurement. Council policy is to install PCs ordered to a standard specification, unless the business case is made to vary this requirement. The standard specification is periodically reviewed and updated.

Disposal of Obsolete/Redundant Equipment

An organisation's data can be compromised through careless disposal of equipment, or materials, such as printed output. It follows then that care must always be taken when disposing of anything which could contain information or data.

If you intend to get rid of any equipment which contains storage media, e.g. fixed hard disks, you must ensure that any sensitive data and licensed software are removed or overwritten prior to disposal. Confidential data on a hard disc may need to be removed either when the disc is replaced or when the computer is made redundant and is available for re-use elsewhere. In the former case the disc should be destroyed. Where the computer is to be passed to another user, care should be taken to ensure that data cannot be read.

Confidential data on removable disks (e.g. External drives, memory sticks, CD/DVD etc) should normally be encrypted, but in any event should be removed if the device is being made available for re-use elsewhere. If they are no longer required they should be destroyed. For advice on this contact the ICT Service Desk.

Damaged storage devices containing very sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

If you have equipment, which is surplus to requirements or no longer useable, contact the ICT Service Desk to arrange for its removal.

Equipment disposal should always be carried out in an environmentally sensitive manner and in line with pertinent regulations. A certificate of destruction should always be obtained for all such disposals.

Disposal of confidential waste

Paper Listings.

Users should be aware that reports generated from computer systems are likely to contain significant amounts of confidential or personal data. Care should therefore be taken that any printed output placed in general waste receptacles do not contain such matter.

Shredding facilities exist at the Civic Centre, Mead Park Depot and various Council offices for confidential waste.

Microfiche

This is becoming increasingly rare, but since microfiche can easily be read it is necessary to destroy the whole fiche, by shredding, incineration or other means.

Other Issues

Starters and Leavers

In order that new starters with the Council are enrolled promptly onto the systems they require, line managers must notify the ICT Service Desk seven days before the new employee begins using the ICT Starters Form. This is available from the ICT Service Desk or in the ICT section of the intranet. This will enable appropriate accounts to be created.

New starters must be made aware of the relevant Council policies, and particularly on proper use of computing services. This policy document should specifically be brought to their attention.

Human Resources will notify ICT of those leaving Council service. When an employee or member leaves the Council, ICT will disable all the relevant user accounts and passwords associated with the individual. Thirty days after this they will be deleted. This deletion will remove all files and e-mails held against that user's personal account.

If any information or data is required from the user account after an individual has left, a request must be made to the ICT Service Desk by the designated management authority, and appropriate access will be given for the limited thirty-day period.

Housekeeping

You should spend time at regular intervals checking through the files you have stored on both your network drives and your hard disk and deleting those which are not required. Do this frequently, and whilst you can still remember what the file was about, rather than waiting until your hard disk or the network drive is clogged up.

Use a sensible system of hierarchical sub-directories to group stored files in a logical structure appropriate to your work. This will ensure that you can find them quickly, and will help you monitor files and spot changes or corruption, which may be caused by a virus.

Remember that all data held by the Council, wherever it is held, could be required in terms of the Freedom of Information Act or the Data Protection Act.

Developing your own systems

If you develop your own systems (using Excel, or Access, for instance), there may come a point where that system has become vital to your work, or to the continuing operation of your service. Many spreadsheets and databases are developed as short term solutions and are deleted at the end of their usefulness, but all too often they grow into full blown systems or databases which, if they go wrong, are extremely difficult to recover.

Make sure that the system has been checked or audited as appropriate by a different person. It is all too easy to develop spreadsheet models, for instance, which contain minor errors in calculation which lead to incorrect information and assumptions.

If your system is likely to be complex, or is intended to be accessible across the network, do register your intention with the ICT Service desk at the outset. It may be that a different method of development could be more appropriate.

Make sure that others, and particularly your manager, are aware of what you are doing. It is imperative that you begin to document your system thoroughly from an early stage, rather than leaving it until the task is too large for the time you can spare.

If your system is designed to be used by others, or is passed on, you should take care to ensure that misunderstandings about its capability are avoided and that adequate training is given.

If your system is becoming too large or difficult to maintain, it may be that you will need support from the ICT Service. Try to identify this early so that any assistance you may require can be scheduled into the ICT development team's plan.

If you have a failure with your developed system, which is critical to your business unit, but ICT are unaware of its existence they may not be able to assist you. It is essential therefore that you register any systems or data sets you may have with ICT (via the Service desk) so that the central software inventory can be kept up to date.