HARBOROUGH DISTRICT COUNCIL

INFORMATION AND COMMUNICATION TECHNOLOGY

SECURITY POLICY

Version 7.0 October, 2011

Peter Rowbotham - Head of Customer
and Community Services

Contents

FOREWORD

Harborough District Council is dependant upon its Information Systems and Technology (IS/ICT) systems for its normal day to day business activities. It is therefore essential for the continued successful operation of the Council that the confidentiality, integrity and availability of its ICT systems and data are maintained at a high level. There is also an obligation on the Council and all employees to comply with relevant legislation such as the Data Protection Acts, the Copyright, Designs & Patents Act and the Misuse of Computers Act.

It follows that a high standard of IT security is required within the Council. To achieve this, the ICT Security Policy has been introduced and everyone who uses the Council's ICT systems or equipment is expected to read it and ensure they comply with its provisions. Negligence in following the procedures stated in this policy may lead to disciplinary action, prosecution and may also render the person personally liable for the cost of replacing or reinstating damaged or corrupt equipment and data.

The policy will be reviewed on an annual basis and updated by the Head of Customer and Community Services.

If you have any doubts about the meaning of any part of this policy, or believe that it could be improved in any way, please contact the Head of Customer and Community Services direct.

Anna Graves, Interim Chief Executive
October, 2011

POLICY OBJECTIVES

The three main objectives of this Security Policy are:

- To ensure adequate protection of the Council's ICT assets, people, programs, data and equipment, on a cost effective basis, against any threat which may affect their security, integrity and /or the level of ICT service required by the Council to conduct its business.

- To ensure awareness amongst the Council's officers and Elected Members of all relevant legislation, and ensure that they fully comply with such legislation.

- To ensure awareness within the Council of the need for IS/ICT security to be an integral part of the day to day operation of the Council's business.

SCOPE

This Information Technology Security Policy will apply to:

- All the Council's employees, Elected Members, contractors and agents.

- All Elected Members of the Council who use the Council's IS/ICT facilities.

- Employees and agents of other organisations who directly or indirectly support the Council's IS/ICT services.

A copy of this policy will be available to all the above.

1. Security Organisation

Objective:

To manage information security within Harborough District Council.

1.1 Responsibilities

The Head of Customer and Community Services is ultimately responsible for all security, and is directly responsible for:

- Reviewing and if appropriate updating the Security Policy.
- Reviewing and monitoring security incidents.
- Agreeing and supporting Council-wide security initiatives.
- Co-ordinating the implementation of the Security Policy across the Council.
- Assigning security roles and responsibilities.
- Monitoring exposure to major threats to information assets.

The security of all hardware situated in service areas is the responsibility of the relevant Head of Service.

The security of all other hardware, Operating Systems, PC applications and corporate software is the responsibility of the Head of Customer and Community Services.

Departmental application software is the responsibility of:

Application	*System Administrator*	*System & Data Owner*
General Ledger, Debtors, Creditors, Bank Reconciliation & Purchasing	Sheila Minton System Administrator	Deputy Chief Executive
Payroll	Sheila Minton System Administrator	Deputy Chief Executive
Revenues and Benefits – Data Only	Leigh Butler Revenues & Benefits Manager	Head of Environment & Leisure Services
Cash Receipting	Justine Baxendale Exchequer Services Assistant	Deputy Chief Executive
Development Control Building Control LDF	Richard Ellis Corporate Services Manager Jack Taylor Building Control Manager Stephen Pointer Policy Manager	Head of Corporate & Development Services
Geographic Information System	Steve Loach Database Administrator	Head of Corporate & Development Services
Environmental Services Commercial Environment Licensing and Enforcement	Ruth Hollingsworth Business Compliance Manager Elaine Bird Community Protection Manager Sarah Greenway Senior Licensing Officer	Head of Health and Enforcement Services
Electoral Registration & Elections	Sheena Mortimer Elections Manager	Head of Corporate & Development Services
Workforce	Kate Evans Human Resources Manager	Head of Corporate & Development Services
Waste Management	Sue Hall Waste Services Officer	Head of Environment & Leisure Services
Land Charges	Sheena Mortimer Elections Manager	Head of Corporate & Development Services
Electronic Records & Document Management	Richard Ellis Corporate Services Manager	Head of Corporate & Development Services
Customer Relationship Management	Rachael Abbott Communications and Consultation Manager	Head of Customer and Community Services
Website & Intranet	Rachael Abbott Communications and Consultation Manager	Head of Customer and Community Services

1.2 Acquisition of Information Systems and Technology

All acquisitions of Information Systems and Technology (IS/IT) for both officers and elected members shall be in accordance with the Council's Procurement Procedures and shall be approved by the Head of Customer and Community Services who shall obtain specialist advice if appropriate.

All new acquisitions of a corporate nature shall be agreed by the Management Board and approved by the Head of Customer and Community Services.

Service area acquisitions shall be agreed between the appropriate Head of Service and approved by the Head of Customer and Community Services.

1.3 Security Information Advice

Specialist advice on information security is available internally from the Head of Customer and Community Services or the ICT Manager.

1.4 Security Incidents

All suspected and actual security incidents experienced by officers or elected members shall be reported immediately to the Head of Customer and Community Services. In the absence of the Head of Customer and Community Services elected members should report incidents to the Chief Executive. In the absence of the Head of Customer and Community Services officers should report incidents direct to the ICT Manager.

It is imperative to identify when a security incident concerns RESTRICTED data as in this event more stringent policies and procedures will need to be followed in a timely manner. Further information on the definition of RESTRICTED is contained in Section 9.2.

Each incident will be investigated and corrective action implemented where appropriate. Any incident that causes serious loss or damage shall also be promptly reported to the relevant Head of Service.

Major security incidents due to failure to follow this policy may be cause for immediate suspension pending a formal hearing, which could result in dismissal.

1.5 Independent Review of Information Security

The content, implementation and practice of this policy will be reviewed independently, to provide assurance that organisation practices properly reflect the policy and that the policy is feasible and effective. Independent reviews will be carried out by the Council's auditors.

2. Security of Third Party Access

Objective:

To maintain the security of organisational IS/IT facilities and information assets accessed by third parties.

2.1 Identification of Risks from Third Party Access

Where there is a business need for third party access to IS/IT facilities and information assets, the security implications and requirements will be determined and controls agreed with the third party.

All new systems will be assessed for risks from third party connections and, where appropriate, controls will be defined in a contract with the third party.

All third party access shall be granted via a secure method. An SSLVPN and 2 factor authentication (2FA) solution is the only mechanism in use for remote access.

A combination of user logon name, password, PIN and token code are required to gain access; the token code is only valid for one remote access session. To control remote access by third parties, e.g. software providers, ICT Services securely retain the 2FA token used to produce the required code to gain access.

Additionally, assigned network accounts' permissions ensure authorised parties can only access relevant Council IS/IT facilities and systems and at agreed times.

All requests for access will be logged by ICT Services.

3. Asset Control

Objective:

To maintain appropriate protection of organisational assets.

3.1 Inventory of Assets

An inventory of IS/IT assets shall be maintained by ICT Services who will promptly update it for all acquisitions and disposals. The accuracy of the inventory shall be verified annually.

4. Personal Security

Objective:

To reduce the risks of human error, theft, fraud or misuse of facilities.

4.1 General

Security roles and responsibilities for all staff, including contractors, using IS/ICT facilities will be included in job descriptions and in contracts where appropriate by the relevant manager. Managers are responsible for ensuring job descriptions or codes of conduct address all relevant security responsibilities.

All potential recruits will be screened by:

- Obtaining two satisfactory references.
- Checking the individual's identity.
- Confirming academic and professional qualifications

4.2 IS/ICT Security Awareness

Objective:

To ensure that users are aware of information security issues and are equipped to comply with the Council's security policy in the course of their work.

All IS/ICT users should be made aware of the correct use of IS/IT facilities in order to minimise possible security risks to the confidentiality, integrity and availability of data or services through user error. Managers are responsible for ensuring such training is provided to their staff as part of the induction programme. All new users will be required to sign the Information and Communication Technology Security Policy (this document) before they are issued with their network user logon name and initial password.

4.3 Responding to Incidents

Objective:

To minimise the damage from security incidents and malfunctions, and to monitor, learn from and reinforce procedures in the light of such incidents.

A security incident shall mean:

- Any event arising from negligence or deliberate inaction that has, or could have, resulted in loss or damage to the Council's ICT systems or data.
- A compromise to the confidentiality, integrity or availability of ICT systems or data.
- An action that is in breach of the security policy.

All security incidents shall be reported immediately to the Head of Customer and Community Services who will instigate an investigation and report any incidents that cause serious loss or damage to their Executive Director and/or the Monitoring Officer.

In the absence of the Head of Customer and Community Services officers should report all incidents to the ICT Manager.

In the absence of the Head of Customer and Community Services elected members should report all incidents to the Chief Executive.

All security incidents will be formally recorded by the Head of Customer and Community Services.

All security incidents involving RESTRICTED data (see definition in 9.2) **must** be reported to the Head of Customer and Community Services, or in their absence to the ICT Manager as in this instance there are set procedures the Council must follow.

A security incident where loss or damage has occurred due to failure of an officer to follow this policy may be cause for immediate suspension pending a formal hearing which could result in dismissal or other disciplinary action.

A security incident where loss or damage has occurred due to failure of an elected member to follow this policy may be cause for investigation by the Monitoring Officer.

5. Physical and Environmental Security

Objectives:

To prevent unauthorised access, damage and interference to IS/ICT services.

To prevent loss, damage or compromise to assets and to the confidentiality, integrity or availability of IT systems or data, and interruption to business activities.

5.1 Secure Areas

IS/ICT facilities such as servers, switches and routers supporting critical or sensitive business activities shall be housed in secure areas, i.e. protected from unauthorised access, damage and interference.

Except for systems specifically intended for public use, IS/ICT facilities should only be available to authorised persons, and wherever possible should be kept away from public access, and preferably view. Anyone unknown to HDC staff working on or with IS/ICT facilities should be challenged. Clarification of the legitimacy of the individual and any work they are performing should be confirmed with the ICT department.

5.2 Equipment Security

IS/ICT equipment and cabling should be protected from spillage or leaks, and must be sited away from where staff or the public walk and also to minimise opportunities for unauthorised access or removal. Staff should also be warned of the dangers of spilling liquids or food on IS/ICT equipment. Except for laptops and portable computers only ICT Services staff should move, or supervise the moving, of ICT equipment.

All servers and critical network equipment shall be protected by an uninterruptible power supply (UPS). UPS equipment should be self testing.

Any faulty IS/ICT equipment shall be reported to the ICT Team who will arrange for its repair or replacement. The Helpdesk response will be within two hours.

Under no circumstances should staff attempt to repair equipment or open casings, except for printing equipment to replace consumables or clear a paper jam.

Computers provided by the council for use at home are for the sole use of that officer or Elected Member, no unauthorised third party is allowed access to the computer equipment for any reason.

Laptop and portable computers and equipment (unless permanently assigned to an officer or elected Member) may be borrowed, from ICT Services with one day minimum prior notice. ICT Services will maintain a record of issues and returns. Such equipment must be transported in appropriate carrying cases, must not be left in clear view in a vehicle or left in an unattended and unlocked vehicle. Equipment should also not be left in a vehicle for extended periods and/or overnight; extremes of temperature may be experienced which could damage the equipment. Officers should ensure that laptops and other portable devices and their data are kept secure at all times. Officers should treat laptop and portable computers and equipment as if it were their own possession and uninsured. It is especially important that equipment containing personal data is kept secure to prevent the data being used for identity fraud or individuals or organisations suffering financial loss.

Removable media (CDs, USB keys etc.) present additional potential exposure for data, officers should follow similar guidelines to those regarding hardware. Media must not be left unattended. For further information please read with the Removable Media Policy.

Users should contact the ICT Helpdesk when they need to transmit data to suppliers.

Any laptops or computers currently assigned on a permanent basis to an officer or Elected Member can be recalled for a software audit on one week's notice. The officer or Elected Member must arrange a mutually convenient time when the computer can be returned to the ICT Service within that week period. Once the audit has been conducted the ICT Service will either return the computer or inform the officer or Elected Member and arrange a collection time and date.

Obsolete equipment shall be checked by ICT Services staff and will be disposed of using a third party where possible for recycling. All hard disks will be cleansed of data and/or physically destroyed before disposal; certificates confirming this will be obtained from the third party.

6. Computer and Network Management

6.1 Operational Procedures and Responsibilities

Objective:

To ensure the correct and secure operation of computer and network facilities.

The ICT Manager is responsible for the management and operation of all servers and networks and associated specialised hardware. Service area managers are responsible for the operation of portable and desktop computers and printers issued to them or their staff.

Appropriate documented procedures for the management and operation of all servers and networks will be established by ICT Services staff.

Clear documented procedures shall be prepared by ICT Services staff and/or the system administrator for all operational computer systems to ensure their correct, secure operation.

6.2 System Planning and Acceptance

Objective:

To minimise the risk of systems failure.

Advance planning and preparation are required to ensure the availability of adequate capacity and resources.

Acceptance procedures for new systems will include the following:

- Performance and computer capacity.
- Preparation of error recovery and restart procedures.
- Preparation and testing of routine operating procedures.
- Evidence that the new system will not adversely affect existing systems, particularly at peak processing times.
- Training in the operation or use of new systems.
- Formal consideration of the need for ongoing maintenance and support by a third party.

Emergency fall back arrangements should be identified for each system and adequate fall back arrangements made wherever possible. Fall back arrangements for each system should be fully documented and responsibility for this lies with the relevant system administrator.

6.3 Configuration and Change Management

Objective:

To document and manage the IS/ICT structure and any changes made thereto.

Operational changes must be controlled to reduce the risk of system or security failures. The Head of Customer and Community Services is responsible for ensuring that changes to software or hardware are carried out in a controlled manner and appropriately documented.

6.4 Protection from Malicious and Unauthorised Software

Objective:

To safeguard the integrity of software and data.

It is essential that special measures, as detailed below, are implemented to prevent the introduction of malicious software such as computer viruses or the use of unauthorised software. Using unlicensed software can result in a raid (authorised by the courts) to identify the use of such unlicensed software, which can result in a fine, adverse publicity and a block on the use of ANY computers until the licences are paid for or the offending software is removed, resulting in very serious disruption to the organisation's activities. In extreme cases staff could face imprisonment. A computer virus or similar can cause severe damage to data and hence serious disruption. Every precaution must be taken to protect Council data and programs.

Unauthorised software is software that has not been purchased by, or whose purchase or use has not been agreed by, the Head of Customer and Community Services or the ICT Manager.

To reduce the risks of infection or use of unauthorised software the following preventive, detective and corrective measures will be instituted:

- The introduction and/or use of unauthorised software, including screensavers, is prohibited and may be treated as gross misconduct.
- Software licences will be complied with at all times.
- Reputable, up to date anti-virus software will be used to detect and remove or isolate viruses.
- Any suspected viruses must be reported immediately to the ICT Helpdesk and, where appropriate, logged as a security incident.
- Do not open e-mail attachments or click on hyperlinks in e-mail from unverifiable sources. Unknown and unexpected e-mail messages pose a significant risk of infection by malicious software; or could be an attempt to obtain personal information (Phishing). If in doubt about the validity of a message, attachment or hyperlink staff should contact the ICT Helpdesk.
- Users must not attempt to download executable files, i.e. program software, from the Internet without prior specific clearance from ICT Services staff.
- Incoming unscannable e-mail messages (e.g. those with password protected compressed files attached) will be automatically blocked and held in

quarantine by our e-mail gateway. Notification will be sent to the intended recipient(s) who will need to respond to the notification e-mail confirming that the message was expected and request that the message is released.

6.5 Housekeeping

Objective:

To maintain the integrity and availability of IT Services.

Housekeeping measures are required to maintain the integrity and availability of services.

Routine procedures will be established by ICT Services staff for taking back-up copies of data, logging events and, where appropriate, monitoring the equipment environment.

Documented procedures for each system shall include:

- Data backup.
- Operator logs.
- Fault logging.
- Environmental monitoring.
- Network and application restart procedures.

6.6 Network Management

Objective:

To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

Appropriate controls must be implemented to ensure the security of data in networks and the protection of connected services from unauthorised access.

Each authorised user will be allocated a unique user logon name by ICT Services staff and a password that they will be prompted to change every 60 days. The password must contain at least seven characters. The password cannot contain your name and must include a combination of characters from three of the following four categories:

- Uppercase letters
- Lowercase letters
- Numbers
- Non-alphanumeric characters (#,&,*,etc.)

Access to the network shall be automatically barred after four successive unsuccessful attempts to logon. Users are responsible for ensuring the secrecy and

quality of their password and shall be held responsible for all actions recorded against their unique logon identifier.

Except in the case of ICT Services staff, no user shall attempt to monitor or analyse network traffic without the specific written agreement of the Head of Customer and Community Services or ICT Manager. Any attempt to do so without such consent shall be treated as gross misconduct.
The Head of Customer and Community Services is responsible for ensuring the security of the networks.

6.7 Media Handling and Security

Objective:

To prevent damage to assets and interruptions to business activities.

Computer media containing data shall be controlled and physically protected. Appropriate operating procedures will be established to protect computer media (tapes, disks, etc.) input/output data and system documentation from damage, theft and unauthorised access.

Staff who regularly need to work with Council data outside of the Council's offices should use a council provided laptop for this. For ad hoc use staff should contact ICT Services and will be issued temporarily with an encrypted memory stick. This should be used to process the data with a non Council PC and the data should not be copied on to alternative storage, e.g. local hard disk.

At least one copy of all computer media containing data or critical software will be stored in media fire safes. A copy of all such media should also be kept securely offsite (in relation to where the backed up system resides). All tapes and disks should be regularly replaced according to accepted norms.

Data held locally on computers that rarely physically connect to the network such as laptops or computers provided to elected Members and some officers are not covered under our backup policy and data backups of these computers is the responsibility of the elected Member or officer. A means of backing up the computer and a lesson on how to backup data can be provided by the ICT Service if required.

Equally staff using computers on the HDC network should also be aware that data held on their local drives is not backed up. Only data on network drives (including users' My Documents folder also known as their G: drive) is covered by ICT's backup procedures.

This should be read in conjunction with the Council's Removable Media Policy.

6.8 Data and Software Exchange

Objective:

To prevent loss, modification or misuse of data.

Exchanges of data or software between the Council and third parties should be managed in accordance with the data classification table in Appendix A.

For critical or sensitive data and software, formal agreements, (including software escrow agreements where appropriate) for exchange of data and software (whether electronic or manual) between organisations should be established.

These agreements should specify appropriate security conditions which reflect the sensitivity of the information involved, including:

- Management responsibilities for controlling and notifying transmission

despatch and receipt.
- § Minimum technical standards for packaging and transmission.
- § Courier identification standards.
- § Responsibilities and liabilities in the event of loss of data.
- § Data and software ownership and responsibilities for data protection, software copyright compliance and similar considerations.
- § Technical standards for recording and reading data and software.
- § Any special measures required to protect very sensitive items.

In order to ensure security of physical media in transit, reliable transport couriers should be used at all times. Packaging should be sufficient to protect the contents from any physical damage during transit, and should be in accordance with manufacturers' instructions.

Data in transit should be sealed with tamper proof or evidence devices, and have accompanying documentation to list package contents.

When providing data electronically to suppliers data should be provided in a compressed password protected file. This will then need to be downloaded by the intended recipient from Harborough District Council's dedicated FTP site; a more appropriate mechanism to exchange large amounts of data.

All electronic commerce should be in accordance with the Council's Constitution and subject to formal contract(s) drawn up between the Council and the trading partner(s), including the specialised areas of communication processes, transaction message security and data storage. Managers will need to obtain the appropriate specialised advice upon, identify and take into account all external and internal requirements affecting this activity. These requirements are likely to include the acts and directives listed in section 9.1 of this policy. Also relevant will be international and local (to other countries) laws and directives, any national or international professional regulations such as accounting practice and tax regimes, any conditions specified by the Council's insurers, fair trade and human rights standards, and the requisite information and technology standards and controls to preserve the timeliness, accuracy and integrity, security, recoverability and processing of this activity.

6.9 Electronic Mail

Objective:

To facilitate use of this means of communication while preventing risks to the Council from inappropriate use.

Controls to reduce the security risks associated with electronic mail (e-mail) should be implemented covering:

- § Vulnerability to unauthorised interception or modification. RESTRICTED data must only be sent via a secure mechanism (i.e. GCSx e-mail account).
- § Users should contact the ICT Helpdesk when they want to send confidential information.

- Vulnerability to error, for example incorrect addressing.
- Legal considerations such as the need for proof of origin, despatch, delivery and acceptance.
- Publication of directory entries.
- Remote access to e-mail accounts.

All staff who have e-mail facilities shall use them in accordance with the Electronic Mail Policy. Users shall avoid responding to unsolicited e-mails from unverifiable sources, and in particular, except where there is a justifiable business reason that has been expressly agreed with the Head of Customer and Community Services, shall not open such mail or any attachments in such circumstances as there is a significant risk they may contain some type of malware.

"Chain" type e-mails should not be forwarded, as they represent another form of spam mail. This type of e-mail is often well known within the IT community, can easily be recognised and validity of claims made within suspect e-mails can easily be checked with ICT Services staff. ICT Services staff shall monitor usage of e-mail and report any concerns to the appropriate line manager or Head of Service.

All e-mail sent to external parties shall contain a standard disclaimer inserted by the e-mail system and in a form approved by the Council's Legal Officer.

6.10 Internet

Objective:

To facilitate use of this major source of information while preventing risks to the Council from inappropriate use.

The use of the Internet on the Council's computer systems by officers and elected members shall be controlled and monitored to prevent:

- Users wasting time and public resources by playing or "surfing" when they are paid to work.
- Users accessing sites and importing material which the Council, as a matter of policy, may find unacceptable.
- Users accessing sites and importing illegal material.
- Users importing a virus or other malicious software and hence compromising the accuracy, availability and confidentiality of Council systems.
- Users committing the Council to expenditure in an unauthorised fashion.

Officers using the internet only access sites relevant to work or vocational training during working hours (this working hours ruling does not apply to elected members).

Outside these hours users may access the Internet for private purposes subject to complying with the Council's Internet Guidelines and their flexi time agreement. All access to the Internet will be traceable to an originating user ID.

All access and attempted access to the Internet will be logged by the ICT Service, and comprehensive information on usage will be supplied on request or in the event

of concerns by the Head of Customer and Community Services, to a user's Head of Service or, in the case of elected Members, the Chief Executive.

The ICT Service will implement and maintain a "firewall" to control and vet incoming data to guard against recognised forms of Internet assaults and malicious software.

Only ICT Services staff may download software, including freeware, from the Internet. This does not apply to documents, e.g. Word, Excel, PDF format.

No user shall attempt to access an Internet site which, from its address, may reasonably be considered to contain pornographic material or any other material prohibited by the Council's Internet Guidelines. Any such attempted access shall be automatically monitored and reported to the user's Head of Service and will be a disciplinary offence.

The Council reserves the right to restrict access to internet sites.

7. System Access Control

7.1 Business Requirements for System Access

Objective:

To control access to business information.

Access to application databases and data should be controlled on the basis of business requirements, but accesses granted to a system should not compromise situations where separation of duties is important.

Each system administrator will set up the system access rights of each user or group of users according to authorised business needs as identified on the new user request form or subsequent request from the individual's line manager. Update access rights should be restricted to the minimum number of people commensurate with the need to maintain service levels.

7.2 User Access Management

Objective:

To prevent unauthorised computer access.

Formal procedures will be developed for each system by the system administrator to cover the following:

- Formal user registration and de-registration procedure for access to all multi-user IT services.
- Restricted and controlled use of special privileges.
- Allocation of passwords to be securely controlled.
- Ensuring the regular change and where appropriate quality of passwords.

- Regular review of user access rights.
- Controlled availability of master passwords.

7.3 User Responsibilities

Objective:

To prevent unauthorised computer access.

Effective security requires the co-operation of authorised users. Users must comply with Council policies, standards and procedures regarding access controls, in particular the use of passwords and the security of equipment.

In order to maintain security users must:

- Not write passwords down.
- Not tell anyone else, including ICT Services staff, their password/s.
- Not use obvious passwords such as their name.
- Use a password with at least seven characters in it. Which doesn't contain your name and must include a combination of characters from three of the following four categories:
  - Uppercase letters.
  - Lowercase letters.
  - Numbers.
  - Non-alphanumeric characters (#,&,* etc).
- After 4 invalid login attempts the account will lockout for 60 minutes.
- Not let other people observe when entering their password.
- Promptly change their password if they suspect anyone else may be aware of it.
- Log out of applications and use the "Lock Computer" options from the Windows Security dialog box (obtained by pressing CTRL + ALT + DEL when logged in) if you will be away from your desk for any length of time.
- Change your password when prompted by the computer (every 60 days).
- Not re-use a password within 20 password changes.

Staff will be held responsible for all activities logged to their unique user ID.

Officers' network account passwords can be reset at the request of their line manager to enable access to e-mail, applications and data in the event of an officer's unplanned absence. These requests must be made in writing (e-mail is sufficient) to the ICT Helpdesk to ensure an audit trail is kept.

7.4 Network Access Control

Objective:

Protection of networked services.

Connections to networked services shall be controlled in order to ensure that connected users or services do not compromise the security of any other networked services.

The Head of Customer and Community Services is responsible for the protection of networked services.

7.5 Computer and Application Access Control

Objective:

To prevent unauthorised access to computers and information held.

Access to computer facilities should be restricted to authorised users. Computer facilities that serve multiple users should be capable of:

- Identifying and verifying the identity of each authorised user, particularly where the user has update access.
- Recording successful and unsuccessful attempts to access the system.
- Providing a password management system which ensures quality passwords.
- Where appropriate restricting the connection times of users.
- Controlling user access to data and system functions.
- Restricting or preventing access to system utilities which override system or application controls.

8. Systems Development and Maintenance

8.1 Security Requirements in Systems

Objective:

To ensure that security is built into IT systems and applications.

All security requirements, including a risk analysis and the need for fallback arrangements, should be identified at the requirements phase of a project by the officer requesting the system in consultation with ICT and audit staff. Security requirements should be justified, agreed and documented.

The analysis of security requirements should:

- Consider the need to safeguard the confidentiality, integrity and availability of information assets.
- Identify controls to prevent, detect and recover from major failures or incidents.

- When specifying that a system requires a particular security feature, the quality of that feature must be specified, e.g. Password controlled - *"the password must be held in encrypted format. Passwords must expire after a number of days set by the system administrator, passwords should not be reusable, the system administrator should be able to specify a minimum length and other rules concerning password composition".*

In order to ensure ICT Services staff and users are aware of security controls in place, controls must be explicitly defined by the relevant system administrator in all relevant documentation.

8.2 Security of Application System Files

Objective:

To ensure that IT projects and support activities are conducted in a secure manner.

Access to application software, data files and system management files should be formalised and documented according to the sensitivity and importance of the system.

Maintaining the integrity of applications is the responsibility of the system administrator who will ensure that:

- Strict control is exercised over the implementation of software on the operational system.
- Test data is protected and controlled.

8.3 Security in Development and Support Environments

Objective:

To maintain the security of application system software and data.

All proposed system changes must be reviewed to ensure they do not compromise the security of either the system or operating environment. The Head of Customer and Community Services is responsible for all operating systems and the appropriate system administrator is responsible for the application. It is essential that both parties work together to ensure the security of application software and data is maintained.

Unsupported modifications to packaged software will only be authorised in exceptional circumstances. Wherever possible the required changes should be obtained from the vendor as standard program updates.

The implementation of any changes to systems should be strictly controlled using formal change control procedures. All system changes will be documented.

It should be as standard that any operational system has separate and secure test/development environments.

9 Compliance

9.1 Compliance with Legal Requirements

Objective:

To ensure compliance with the following statutes which impose criminal or civil obligations.

There are a number of laws which relate directly or indirectly to IT and its use and it is essential that these statutory requirements are met. Legislation which applies includes:

The Copyright, Designs and Patents Act 1988
The Data Protection Act 1998
The Computer Misuse Act 1990
Health and Safety at Work etc. Act 1974
EC Directives

9.1.1 Control of Proprietary Software Copying

Proprietary software is usually supplied under a licence agreement which limits the number of users and/or limits the use to a specified machine. Copyright infringement can lead to legal action, fines and adverse publicity.

It is Council policy that no copyright material is copied without the owners consent.

9.1.2 Use of Unlicensed Software

Except for freeware, the use of unlicensed software amounts to theft and the Council's policy is only to use licensed software. The Federation Against Software Theft (FAST) and the Business Software Alliance are particularly active in detecting and prosecuting organisations (especially Councils) who use unlicensed software. The introduction and/or use of unlicensed software is prohibited and may be treated as gross misconduct.

9.1.3 Safeguarding of the Council's Records

Important records must be protected from loss, destruction and falsification. The "Retention (Document and Disposal)" policy is available on the intranet and provides guidance for departments.

9.1.4 Data Protection

Personal information on living individuals who can be identified from the information that is stored or processed on a computer is subject to data protection legislation. The Data Protection Act 1998 extended this to information held in certain paper based systems. Disclosure of information is also governed by the Freedom of Information Act 2000.

Removable media (CDs, USB keys etc.) present additional potential exposure for data, officers should follow similar guidelines to those regarding hardware. Media must not be left unattended. It is especially important that personal data is kept secure to prevent the data being used for identity fraud or individuals or organisations suffering financial loss.

When providing information for suppliers data should be provided in a password protected zip file. This will then need to be downloaded by the intended recipient from a dedicated FTP; a more appropriate mechanism to exchange large amounts of data.

Users should contact the ICT Helpdesk when they need to transmit data to suppliers.

Data portability and remote access to applications and data presents considerable security risks. Further information is contained in sections 9.2 including transport of RESTRICTED data and access to it from abroad.

The officer responsible within the Council for data protection is the Head of Customer and Community Services who will provide guidance to managers and other staff on their individual responsibilities and the specific procedures that should be followed.

It is the Head of Service's responsibility to inform the Head of Customer and Community Services of any proposals to keep personal information on a computer and any changes in the use for which data is kept and to ensure awareness of the data protection principles defined in the legislation.

The Council is required to register details of the data kept, the purposes to which it is applied and to whom it may be disclosed. It is the Head of Service's responsibility to ensure that the registration is accurate and amended when necessary and to take note of any advice from the Information Commissioner before undertaking any data matching exercise.

Under the Act, staff could be held legally responsible for the confidentiality of personal data. Staff must be very careful as to whom they disclose information and be aware of the need for security of printouts. Particular care must be taken in disclosing personal data on the telephone, if in any doubt as to the identity of a caller personal data must not be disclosed on the telephone.

The eight principles of the Data Protection Act are that personal data should be:

- Processed fairly and lawfully.
- Obtained only for specified lawful purposes and shall not be further processed in any manner incompatible with those purposes.

- Adequate, relevant and not excessive.
- Accurate and where necessary kept up to date.
- Not kept longer than necessary.
- Processed in accordance with the rights of data subjects under the Act.
- Protected against unauthorised or unlawful processing and against accidental loss, destruction or damage by appropriate technical and organisational measures.
- Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

9.1.5 Prevention of Misuse of IT Facilities

The Council's computer facilities are provided for Council business or in connection with approved study courses. Staff and elected Members are allowed to use the Council's computer facilities for personal use for the following:

- Personal use of e-mail in accordance with the E-mail Usage Policy.
- Access to the Internet in accordance with the Internet Usage Policy.
- Limited use of PC software, particularly word processing, in their own time.

Unauthorised or excessive personal use may be subject to disciplinary action.

The Computer Misuse Act 1990 introduced three criminal offences;

- Unauthorised access.
- Unauthorised access with intent to commit a further serious offence.
- Unauthorised modification of computer material, i.e. alteration, erasure or addition to programs or data.

Users should not attempt to gain access to systems they are not authorised to use or see, as they could face criminal prosecution.

9.2 Access to RESTRICTED information

Certain departments working in partnership with Central government and other national bodies and agencies have a requirement to exchange and share information requiring protection and handling in line with the requirements of the Central Government Manual of Protective Security (MPS). An example being the Benefits department and their use of DWP data.

Protective marking is allocated an appropriate Impact Level (IL) describing the severity of impact of the information being released outside of normal government channels.

Protective Marking	e-Gov Impact Level
TOP SECRET	6
SECRET	5
CONFIDENTIAL	4
RESTRICTED	3
PROTECT	2 1
Unclassified	0

It is envisaged (by Central Government) that the majority of protectively marked information shared or exchanged with Local Authorities will be of the “PROTECT” type.

RESTRICTED information is defined as any asset whose compromise would be likely to:

- Adversely affect diplomatic relations.
- Cause substantial distress to individuals.
- Make it more difficult to maintain the operational effectiveness or security of UK or allied forces.
- Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies.
- Prejudice the investigation or facilitate the commission of crime.
- Breach proper undertakings to maintain the confidence of information provided by third parties.
- Impede the effective development or operation of government policies.
- Breach statutory restrictions on the disclosure of information (except the Data Protection Act – which can be addressed by other impact statements and/or the e-Government Security Framework).
- Disadvantage government in commercial or policy negotiations with others.
- Undermine the proper management of the public sector and its operations.

Staff handling RESTRICTED data must be briefed by their Line Management prior to being allowed access. ICT Services will only allow access to potentially RESTRICTED data on receiving a signed Personal Commitment Statement (available within the Policies and Procedures section of the intranet).

An important note is that when dealing with Central Government CONFIDENTIAL is an explicit marking with specific handling requirement so care must be taken to ensure confusion is not caused by its use.

If using ICT facilities whilst outside of the United Kingdom systems with RESTRICTED data must not be accessed.

PROTECT and RESTRICTED markings will be the most commonly seen protective markings, with the former being the most prevalent. Data of both markings will be handled the same in most circumstances with the main difference that information

protectively marked as RESTRICTED is not allowed to be passed over the telephone.

Further guidance, if required, should be sought from the Head of Customer and Community Services.

9.3 Security Reviews of IT Systems

Objective:

To ensure compliance of systems with Council security policies and standards.

The security of IT systems will be regularly reviewed.

This review will be carried out by Internal Audit, External Audit, managers and the Head of Customer and Community Services who may use specialist third parties. Reviews will ensure compliance with the security policy and standards.

9.4 System Audit Considerations

Objective:

To minimise interference to/from the system audit process.

Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes. There should be controls to safeguard operational systems and audit tools during system audits.

The following are to be observed:

- § Audit requirements to be agreed with the appropriate manager.
- § The scope of any checks to be agreed and controlled.
- § Checks to be limited to read only access to software and data wherever possible.
- § Access, other than read only, only to be allowed for isolated copies of system files which must be erased when the audit is completed.
- § ICT resources for performing checks should be identified and made available.
- § Requirements for special or additional processing should be identified and agreed with service providers.
- § Wherever possible access should be logged and monitored.
- All procedures and requirements should be documented.
- Access to system audit tools should be controlled.

9.5 PCI DSS - Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) must be met by all organisations that transmit, process, or store payment card data. The Council accepts face to face, online and telephone payments from its customers and is therefore required to demonstrate compliance with the requirements of PCI DSS.

PCI DSS security requirements apply to all system components. This includes any network component, server or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that processes cardholder data or sensitive authentication data.

When the Council accepts a payment card transaction, a complex system of devices, software, networks, service providers and the card acquirer is required to process the payment and obtain the money. Each element of the payment card technology system poses risks that could be exploited by criminals; therefore, it is important to use appropriate security controls and business procedures to minimise risk and protect cardholder data.
The Council cannot control the entire payment card system; therefore, PCI DSS limits the scope of responsibility to protecting cardholder data with security technologies and processes that cover the Councils' domain.

The table (on the next page) illustrates commonly used elements of cardholder and sensitive authentication data; whether storage of each data element is permitted or prohibited; and whether each data element must be protected.
This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

PCI DSS requirements are applicable if a Primary Account Number (PAN), which is the 14-16-digit numeric code embossed on the face side of a payment card, is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.

	Data Element	Storage Permitted	Protection Required*	Rendered Unreadable
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name[1]	Yes	Yes[1]	No
	Service Code[1]	Yes	Yes[1]	No
	Expiration Date[1]	Yes	Yes[1]	No
Sensitive Authentication Data[2]	Full Magnetic Stripe Data[3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

[1] - These data elements must be protected (such as through the use of encryption and / or logical access) if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

[2] - Sensitive authentication data must not be stored after authorization (even if encrypted).

[3] - Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

* - The Council must always render the PAN unreadable wherever it is stored, including in backup media, in logs, on portable digital storage devices, and via wireless networks.

Permissible technology solutions for masking PAN include:

- Strong one-way hash functions or a hashed index, which shows only index data that points to database records containing the PAN.

- Truncation, which deletes a forbidden data segment and shows only the last four digits of the PAN.

- Strong cryptography and associated key management processes and procedures. Cryptographic keys must be protected from disclosure and any misuse documented by the Council.

9.5.1 Security Awareness Training

The Council rolled out an eLEarning portal (Learning Pool) to all staff in 2010/11. Courses relating to ICT security (including PCI DSS) are in the catalogue of courses available. Users who process payment card details will be required to complete appropriate training; further information regarding this can be obtained from the Learning & Development Officer.

9.5.2 Technical Network Testing

The PCI DSS standard requires the Council to regularly test cardholder data systems and processes, in order to systematically identify vulnerabilities and accordingly address them.

Items to test include wired and wireless networks, network hardware, servers, other system components, processes, and custom software.
Testing must be frequent, and is important right after the Council makes big changes such as deploying new software or changing system configuration.

The PCI DSS requirements include the following technical testing:

- A quarterly test for the presence of unauthorised wireless access points [PCI DSS requirement 11.1].

- Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). [PCI DSS requirement 11.2].

- Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (this testing does not need to be conducted by an ASV). [PCI DSS requirement 11.3]

The Council has a vulnerability scanning policy to comply with PCI DSS, as well as the Government Connect Code of Connection, requirements. Internal checks are performed by ICT Services staff on newly implemented systems and regular external penetration tests and internal IT HealthChecks are performed by suitably accredited 3rd party suppliers.

9.6 ISO IEC 27001:2005 Information Security Standard

BS 7799 was a standard originally published by the British Standards Institution (BSI) in 1995. It was written by the Department of Trade and Industry (DTI) and consisted of several parts.

The first part of the standard contains the best practices for Information Security Management. ISO/IEC 17799 was revised in June 2005 and finally incorporated in the ISO 27000 series of standards as ISO IEC 27002 in July 2007. The standard focuses on how to implement an information security management system (ISMS) referring to the information security management structure and controls identified in BS 7799-2, which later became ISO IEC 27001. An ISMS is the means by which Senior Management monitor and control information security, minimising the residual business risk and ensuring that security continues to fulfil corporate, customer and legal requirements. It forms part of an organisation's internal control system.

The Council has not sought full accreditation to the standard, however it attempts where possible to comply with its requirements. Parts 1 and 2 of the standard provide a set of key controls considered necessary to comply with the standard and detailed guidance to assist with the implementation of information security. The areas of the Standard that the Council seeks to comply with are as follows:

- An officer with formal responsibility for information security.
- Information security training and information security awareness programmes are provided for computer users.
- The Council has approved the following information security related policies:
  - ICT Security Policy (this document).
  - Internet and E-mail Acceptable Use Policy.
  - Information and Data Retention and Disposal Policies.
- The Council has formal processes to manage the users of its corporate network and information systems.
- The Council has approved IT change management and change control procedures.
- The IT Department carries out security monitoring and auditing of its main IT systems.
- The IT Department is responsible for ensuring that all Council laptops are correctly configured and secure for use.
- There is a policy in place for network and systems penetration testing and vulnerability management.
- The Council has IT disaster recovery and business continuity processes in place

Appendix A

Data Classification Table

Class Medium	Of Particular Sensitivity	Commercial Confidential	Personal Confidential	Council "Business"	Public Domain
Print	To be subject to a clear desk policy. Not to be photocopied. To be marked appropriately. To be stored securely (e.g. safe) or in secure premises.	To be subject to a clear desk policy. To be restricted to authorised staff.	To be subject to a clear desk policy. To be restricted to authorised staff. To be registered for data protection purposes.	To be subject to a clear desk policy.	No restriction
Internal Distribution	To be personally delivered in an appropriately marked and sealed envelope.	In sealed envelope marked private and confidential.	In sealed envelope marked private and confidential.	In internal envelope.	No restriction
External Distribution	Delivery by self, or sealed for Council staff to deliver, or in registered package via courier.	In sealed envelope marked private and confidential.	In sealed envelope marked private and confidential.	Always in a sealed envelope.	No restriction
Telephone	Not to be discussed on mobile phone in public area.	Not to be discussed on mobile phone in public area.	Not to be discussed on mobile phone in public area.	No restriction	No restriction

Data Classification Table (continued)

Class Medium	Of Particular Sensitivity	Commercial Confidential	Personal Confidential	Council "Business"	Public Domain
Fax	To be transmitted on attend basis only.	To be transmitted to fax in recipient's area or section.	To be transmitted to fax in recipient's area or section.	No restriction	No restriction
Hard Disc	To be encrypted to an appropriate standard. Application and network to be secured, review data/system location and accessibility.	Application and network to be secured.	Application and network to be secured.	Application and network to be secured.	To be read only (by public)
Internet & external e-mail	Not advised. If sent to be encrypted to an appropriate standard.	To be encrypted to an appropriate standard.	To be encrypted to an appropriate standard.	No restriction	No restriction
Removable Media e.g. USB Memory Stick , CD/DVD	Not advised.	Not advised.	Not advised.	To be kept securely.	No restriction.

ICT Policy Documents Agreement

I have read the Council's "E-mail Policy", "Internet Usage" and "ICT Security Policy" documents, fully understand the terms and conditions and agree to abide by them.

I understand that the Council's security systems will record for management use all Internet / Intranet and Electronic Mail activity undertaken by me, including the addresses of web sites visited or attempted to be visited and any material transmitted or received.

I understand that violation of this policy may lead to disciplinary action, including termination of employment, and could also lead to personal criminal prosecution.

I herby certify that I have read and understood everything contained within the ICT policy documents listed above and will abide by their contents.

User:

Full Name: .....

Signature: ..... Date: .....

Head of Service or Line Manager:

Full Name: .....

Signature: ..... Date: .....

In order to use HDC ICT equipment or access the HDC network this form needs to be completed and returned to ICT Services.