

ICT Security Policy



EAST RIDING
OF YORKSHIRE COUNCIL

Lead Directorate and Service:	Corporate Resources - Digital Change and Technology
Effective Date:	December 2022
Contact Officer/Number:	David Cox - ICT Security Manager
Approved By:	The Cabinet

Contents

ICT Security Policy.....	1
1. Introduction.....	1
2. Definitions for the Purposes of this Policy.....	1
3. Policy Statement.....	1
4. Policy Statement.....	1
5. Scope.....	2
6. Corporate Requirements	2
7. Policy Development including Consultation	2
8. Links with Other Policies	2
9. Standards and Procedures.....	3
10. Policy Compliance.....	5
11. Financial Implications	5
12. Review	5
ICT Access to ICT Resources - Appendix 1	6
ICT ICT Information Protection - Appendix 2	9
ICT ICT Operational Management - Appendix 3	11
ICT ICT remote Working - Appendix 4	16
ICT ICT Software - Appendix 5	18

Cyber Incident Response Policy

1. Introduction

East Riding of Yorkshire Council (the Council) is aware that all ICT systems and data information assets are of paramount importance in supporting and enabling the Council's strategic objectives. The Council recognises its obligations to protect information from internal and external threats and recognises that effective information security management is critical in order to ensure the successful enablement of ICT and the delivery of business functions and services.

The Council is committed to preserving the confidentiality, integrity, and availability of all physical and electronic assets. Information security management is an ongoing cycle of activity aimed at continuous improvement in response to emerging and changing threats and vulnerabilities. It can be defined as the process of protecting information from unauthorised access, disclosure, modification or destruction and is vital for the protection of information and the Council's reputation.

2. Definitions and Purposes of this Policy

For the purpose of this Policy the key definitions are:

ICT Security: the products, services, organisational rules and expected individual behaviour put into place in order to protect the Council's ICT systems and equipment from unauthorised use.

Information Security: the protection of information held or processed on Council ICT systems against accidental or malicious disclosure, modification or destruction.

3. Policy Objectives

The main objectives of this Policy are to:

- protect the Council's information and prevent data losses
- protect its ICT systems and information assets from threats that compromise their effectiveness
- ensure that users are aware of and fully compliant with all relevant legislation
- create and maintain a level of awareness of the need for information security to be an integral part of daily operations, so that all users of ICT systems understand the need for information security and their own responsibilities
- ensure the security of data we share both in transit through the use of encryption and through due diligence on the organisations we share with

4. Policy Statement

The Council will:

- establish specific requirements for protecting information and information systems against unauthorised access
- effectively communicate the need for access control of information and information systems access control
- ensure that information is available in a timely manner and can be restored in the event of a physical or technical incident
- have in place a process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring security.

5. Scope

The ICT Security Policy applies to all information assets including:

- All ICT systems belonging to, or under the control of the Council
- Information stored or used in Council ICT systems
- Information in transit across the Council's voice or data networks
- Control of information leaving the Council
- All parties who have access to, or use, of ICT systems and information belonging to the Council or under its control

This Policy applies to all employees, Councillors, committees, partners and contractual third parties and agents of The Council who access and use Council-owned ICT facilities and equipment.

6. Corporate Requirements

ICT Security is vital to the effective operation of the Council. All ICT systems used by the Council must adhere to the highest standards of ICT security at all times so that:

- The public and all users of the Council's information systems are confident of the confidentiality, integrity and, availability of the information used and produced.
- Business damage, interruption and damage to reputation caused by security incidents are minimised.
- All legislative and regulatory requirements are met.
- The Council's ICT equipment and facilities are used responsibly, securely and with integrity at all times.

7. Policy Development including Consultation

This Policy has been developed in consultation with:

- Corporate Management Team
- Senior Management Team

- Information Governance Management Board
- Portfolio Holder
- Head of Digital, Change and Technology
- Head of Legal and Democratic Services and Senior Information Risk Owner (SIRO)
- Head of People Services
- Data Protection Team
- ICT Management Team
- ICT Security Manager

8. Links with Other Policies

The following Council Policy documents are directly relevant to this Policy and are referenced within this document:

- Information Management Strategy
- ICT Strategy and Technical Framework
- ICT Acceptable Use Policy
- Policy and Guidelines on the use of electronic mail (eMail)
- Policy and Guidelines on the use of the Internet
- Records Management Policy
- Use of Council resources
- Data Protection Policy
- Cyber Incident Response Policy
- ICT BYOD Policy
- ICT Firewall Change Management Policy
- ICT Patch Management Policy
- Third Party ICT Access Policy
- Policy and Guidance for Web Application Penetration Testing

9. Standards and Procedures

9.1 Access to ICT Resources

Precautions must be taken to ensure that access to desktop and laptop PCs, tablets and smartphones is restricted at all times to authorised personnel.

When equipment is left unattended for an extended time, such as overnight, it must be powered off. Mobile equipment, such

as laptops, tablets and smart phones, must be locked away in offices and never left on view in unattended vehicles.

All appropriate computer equipment will be identity-tagged and be recorded on the Council's IT asset inventory. It is the responsibility of service area managers to notify the IT service desk of any movements or changes.

No equipment purchased, leased or hired by a user department may be connected to the Council's network or attached to any equipment connected to the network without authorisation from the ICT Service.

The ICT Service should be asked to review the specification of any technology that requires additional devices or software to be connected or run on the Council's network before it is ordered.

M365 Office functionality is available to personal iPhone/iPad and Android phone and tablet users and will be operated in accordance with the Council's separate Bring Your Own Device Policy.

Only removable media devices supplied by the ICT Service may be used to store Council data unless permission is granted by the ICT Service.

All classified personal and sensitive data stored on removable media must always be encrypted

The following precautions should be taken to ensure that only authorised personnel have admission to office areas where there is access to ICT systems or sensitive data:

- employee badges should be worn and be visible at all times
- visitor procedures should be followed
- where Principles of Occupation exist for offices, staff should adhere to any relevant clear desk policies to ensure

sensitive data is protected when desks are left unattended.

Key Messages

- All users must use strong passwords
- Passwords must be protected at all times
- User access rights must be reviewed at regular intervals
- It is a user's responsibility to prevent their username and password being used to gain unauthorised access to Council systems

[For full details refer to ICT Access - Appendix I](#)

9.2 ICT Information Protection

The Council will ensure the protection of all information assets within its custody.

High standards of confidentiality, integrity and, availability of information will be maintained at all times.

Key Messages

- The Council must develop and maintain retention inventories of all important information assets.
- Line Managers must ensure that staff only have access to information assets, systems and services pertinent to their current role. This will conform to the principle of least privilege so that employees are only permitted access to information and resources that are required for the role.
- All classified personal and sensitive data that is held locally on laptops, hard drives, memory sticks etc must be encrypted. Further guidance is provided in the Information Protection Assessment guide.

[For full details refer to the ICT Information Protection section 2](#)

9.3 ICT Operational Management

All devices (including laptops and tablets) are protected by anti-virus and anti-malware protection software which is upgraded and monitored regularly by the ICT Service. Any detected or suspected malicious activity must be reported to the ICT service desk immediately.

Key Messages

- Changes to the Council's IT operating systems must follow the Council's formal change control procedure.
- Unpatchable and unsupported software must not be used unless specific permission is granted by the ICT Service and signed off by the Council's Senior Information Risk Owner (SIRO) either with mitigation or as an accepted risk.
- Appropriate access controls must be put in place to prevent user installation of software and to protect against malicious mobile code.
- Regular backups of essential business information are taken to ensure that the Council can recover from a disaster or media failure.
- Storage media must be handled, protected and disposed of with care in accordance with the disposal procedures.

[For full details refer to the ICT Operational Management – Appendix 3](#)

9.4 ICT Remote Working

The Council provides users with the facilities and opportunities to work remotely as appropriate. The Council will ensure that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.

Key Messages

- It is the user's responsibility to safeguard and to use portable computer devices in an acceptable way. Users must always take due care and attention when moving portable computer devices.
- Users should be aware of the physical security dangers and risks associated with working in any remote office or mobile working location.
- It is the user's responsibility to ensure that access to all information is controlled – e.g. through password controls.
- All data held on portable computer devices must be encrypted unless explicit prior approval has been granted in writing from the ICT Service.

[For full details refer to the ICT Remote Working - Appendix 4](#)

9.5 ICT Software

The Council will ensure the acceptable use of software by all users of the Council's computer equipment or Information Systems.

Key Messages

- All software acquired must be purchased through the departmental IT Business Analysts.
- All software on a Council-owned computer is required to be licensed to the Council.
- Unauthorised changes to software must not be made.
- Personal or unauthorised software must not be loaded onto a council machine.
- Users must not attempt to disable or reconfigure any software updates that have been installed to protect the device.
- Illegal copying of software is not permitted and is subject to civil damages and criminal penalties.

- It is the user's responsibility to install all software updates when prompted to do so

[For full details refer to the ICT Software - Appendix 5](#)

10. Policy Compliance

If any user is found to have breached this Policy, they will be subject to the Council's disciplinary procedures. If a criminal offence is considered to have been committed, further action may be taken to assist in any subsequent criminal investigation.

If you do not understand the implications of this Policy or how it may apply to you, seek advice from your line manager or the IT Service Desk.

11. Financial Implications

The requirement to ensure appropriate protection of the Council's corporate infrastructure is one that can be managed within existing budgets.

12. Review

This Policy will be reviewed on an annual basis unless there are major changes or a security-event, then the Policy will be reviewed after the event has been resolved.

APPENDIX I**ICT Access****I. Passwords****I.1. Choosing Passwords**

Passwords are the first line of defence for our ICT systems and together with the user ID help to grant appropriate user access.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

The Council has a password reset self-service facility that should be used in the first instance.

I.2 Weak and strong passwords

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

User Passwords must

- be at least 9 characters long
- include three of the following
 - numbers
 - upper case letters
 - lower case letters
 - other characters such as !, £, \$, and %.
- be changed at least every 90 days
- not include parts of or all of the user's name
- not have more than two consecutive characters the same

Privileged Domain Passwords must

- be at least 15 characters long
- include three of the following
 - numbers
 - upper case letters
 - lower case letters
 - other characters such as !, £, \$, and %.
- be changed at least every 180 days
- not include parts of or all of the user's name

1.3 Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered:

- Never reveal your passwords to anyone
- Never use the remember password function
- Never write your passwords down or store them where they are open to theft
- Never store your passwords in a computer system without encryption
- Do not use any substantial part of your username within the password
- Do not use the same password for systems inside and outside of work
- Do not email passwords
- Use different passwords from those used to access the Council's network and systems for device specific passwords, i.e. encrypted memory Sticks

1.4. Changing Passwords

All user-level passwords must be changed at least every 90 days, or whenever a system prompts you to change it. Default passwords must be changed immediately it is used for the first time. If you become aware, or suspect, that your password has become known to someone else, you must change it immediately and report your concern to the IT Service Desk.

Users must not reuse the same password within 20 password changes.

1.5 System Administration Standards

The password administration process for individual Council systems is well-documented and available to designated individuals. Further information can be obtained from the relevant System Administrator.

All Council IT systems are configured, where possible, to enforce the following:

- Authentication of individual users, not groups of users - i.e. no generic accounts
- Protection with regards to the retrieval of passwords and security details
- System access monitoring and logging - at a user level
- Role management so that functions can be performed without sharing passwords
- Password administration processes are properly controlled, secure and auditable

2. Employee Access

2.1 User Access Management

Formal user access control procedures must be documented, implemented, and kept up-to-date for each IT application and information system to ensure authorised user access and to prevent unauthorised access. The procedure must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. The de-registration of leavers must be in accordance with the Council's starters and leavers process. Each user must be allocated access rights and permissions to computer systems and data that:

- Are appropriate to the tasks they are expected to perform
- Have a unique login that is not shared with or disclosed to any other user
- Have an associated unique password that is requested at each new login

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

2.2 User Registration

A request for access to the Council's corporate network and corporate systems must first be submitted to the IT Service Desk for approval. For access to the Council's directorate-based applications a request must be made to the relevant IT Systems Administrator. All requests for access must only be submitted if approval has been gained from the employee's line manager.

When an employee leaves the Council or changes roles within the Council, their access to computer systems and data must be withdrawn in accordance with the starters/leavers process available on the intranet. For leavers this will be at the close of business on the employee's last working day and it will be reviewed for employees who are changing roles. It is the responsibility of the line manager to request the suspension or removal of corporate access rights via the IT Service Desk and inform the appropriate Systems Administrator for directorate-specific systems.

APPENDIX 2

ICT Information Protection

1 Identifying Information Assets

The process of identifying important information assets should be proportionate and pragmatic. The Council must draw up and maintain retention inventories of all important information assets as detailed in the Council's Records Management Policy.

2 Classifying Information

The way the Government identifies the security level of its information, is called the Government Protective Marking Scheme (GPMS). The Council follows this marking scheme to ensure it continues to share its information securely.

The Council will implement the three marking schemes shown below:

Marking Scheme Descriptor	Usage
Not Sensitive	This is the default option with no impact on the document
Official-Sensitive	Personal and commercially sensitive information is marked internally. Classification marking option within M365: Any document chosen to be classified with this marking option, will have a watermark applied on each page notifying the reader that it is a sensitive document
Official-Sensitive (individual)	Classification marking option within M365: Documents with this label are encrypted and there are a number of options available that restrict how a document can be used. Those granted access will be allowed to see its contents

You should refer to Protective Marking of Information Guidance document, located on the Intranet for full details on the application of information classification.

3 Information Storage

All electronic information will be stored on centralised facilities to allow regular backups to take place.

Records management and retention guidance will be followed as detailed in the Council's Records Management Policy.

Staff must not be allowed to access information until their line manager is satisfied that they understand and agree the legislative responsibilities for the information that they will be handling.

Databases holding personal information will have a defined security and system management procedure for the records and documentation.

Information which has been classified Official-Sensitive or is deemed personal or sensitive information must not be stored on any removable device or portable device (e.g. laptop, netbook or tablet PC) unless the device is encrypted.

For the majority of users, protection on portable PCs is provided by using a product such as TrueCrypt. However, where access could be granted to Official-Sensitive data using the Public Services Network (PSN) all portable PCs must be encrypted using a compliant FIPS 140-2 encryption system

4 Data Integrity

Data integrity refers to the accuracy and reliability of data. Data integrity can be compromised in a number of ways including:

- Human error when data is entered
- Errors that occur when data is transmitted from one computer to another
- Software bugs or viruses
- Hardware malfunctions, such as disk errors or corruption

It is the responsibility of every individual to ensure that the information they manage, or process is correctly verified as detailed in the Records Management Policy.

APPENDIX 3**ICT Operational Management****I Operational Procedures and Responsibilities****I.1 Documented Operating Procedures**

Operating procedures are used in all day-to-day maintenance of the Council's IT systems and infrastructure in order to ensure the highest possible service from its assets. These operating procedures must be documented to an appropriate level of detail for the departmental team that will be using them and in support of services business continuity arrangements.

I.2 Change Management

Changes to the Council's operational systems are controlled by a formally documented change control procedure. The change control procedure should include references to:

- A description of the change and business reasons
- Information concerning the testing phase
- Impact assessment including security, operations and risk
- Formal approval process
- Communication to all relevant people of the changes
- Procedures for aborting and rolling back if problems occur
- Process for tracking and audit

All significant changes to the main infrastructure (e.g. Network, Directories) need to be assessed for their impact on information security as part of the standard risk assessment.

All changes to corporate systems or infrastructure must be approved by ICT Service. Changes to directorate applications must be approved by the appropriate named officers as detailed on the Request for Change (RFC) list.

I.3 Separation of Development, Test and Operational Facilities

The development and test environments must be separate from the live operational environment to reduce the risk of accidental changes or unauthorised access. The environments should be segregated by the most appropriate controls including, but not limited to, the following:

- Running on separate computers and instances
- Different usernames and passwords that do not have administrator rights

2 System Planning and Acceptance**2.1 Capacity Planning**

All the Council's IT infrastructure components or facilities are covered by capacity planning and replacement strategies provided by the Council's IT service provider to ensure that increased power and data storage requirements can be addressed and fulfilled in a timely manner.

Key IT infrastructure components include, but are not restricted to, the following:

- Servers - including data, application, hosts, web, domain servers
- Storage
- Licensing
- Databases
- Networks – all aspects including bandwidth
- Environmental controls including air conditioning
- Citrix/MyWorkSpace
- Multi-Factor Authentication (MFA)

2.2 System Acceptance

All departments must inform the appropriate IT Business Analysts and the ICT Service via the IT Service Desk of any new product requirements or of any upgrades, service packs, patches or fixes required to existing systems. All new products must be purchased through the directorate IT Business Analysts or a member of the ICT Service.

New information systems, product upgrades, patches and fixes must all undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented, and must involve ICT Service authorisation using the Change Authorisation process.

Third party applications must also be monitored for service packs and patches.

Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test environment that duplicates the operational system.

2.3 Cloud Computing and Externally Hosted Systems

As more services move into the cloud or are hosted externally there is an increased risk that business critical IT Systems become more reliant on third party infrastructure and the Council's own Internet connectivity.

It is the responsibility of service managers to ensure that all business critical IT systems and services hosted externally or in the cloud are detailed on the IT Service Desk and that support agreements are in place to provide the appropriate level of support and availability.

With the increased use of Cloud-based servers becoming more prevalent, it is essential that all service areas are aware that all procurement of new IT related systems are approved by the ICT Service.

The security standards of any hosted or cloud offering do not differ in terms of system security for any system that involves the use and transmission of Council-owned data information. In simple terms Information Security follows three basic tenets, as follows:

- Confidentiality: information is only being seen or used by people who are authorised to access it.
- Integrity: any changes to the information by an unauthorised user are impossible (or at least detectable), and changes by authorised users are tracked.

- **Availability:** the information is accessible when authorised users need it.

If the system under scrutiny conforms to these standards, then it is deemed secure. A technical solution must be mindful of the constantly changing technical security standards and this will need to be built into the solution. The means, for example, if an encryption standard changes or a vulnerability to the operating platform is detected the supplier must undertake any remedial action needed to maintain the Confidentiality, Integrity and Availability of information.

When a cloud based/hosted solution is procured the ICT Service will evaluate the vendor solution based on CESG Cloud Security Principles. Points or questions arising from these principles should be included in the method statements for the tender bid. Therefore, it is likely that the answers will be technically complex and may need additional follow up by the ICT Service

The CESG Cloud Security Principles (14 August 2014) were adopted by the NCSC and updated in September 2016. The NCSC Updated Cloud Security Principles are on the NCSC web page for further clarification and guidance on the requirements for each security principle.

The Council, as a member of the Yorkshire and Humber Warning, Advice and Reporting Point (YH-WARP), in conjunction with a representative from the NCSC, have further collaborated to produce a hosted / cloud security response template that suppliers must complete as a part of the procurement process.

2.4 Multi-Factor Authentication (MFA)

Utilising MFA is one of the most effective ways to protect systems from credential based cyber-attacks. This is an essential step as a minimum for all Internet accessible systems that are accessible for employee access as well as administrative purposes via username and password only.

This MFA approach applies to both on-premise and cloud hosted systems that have access, store or process Council resources. MFA should be applied to any system that contains personal, confidential or restricted data or that requires an additional layer of protection if the system could be utilised as an attack vector.

3 Protection against Malicious Code

Appropriate steps are taken to protect all the Council's IT systems, infrastructure and information against malicious code. Effective and up-to-date anti-virus and end-point protection software is run on all servers and PCs. Council IT staff are responsible for ensuring that they do not introduce malicious code into The Council IT systems.

Where a virus is detected on a Council system, the individual must immediately report it to the IT Service Desk.

3.1 Controls against Malicious Code

In order to prevent malicious code, appropriate access controls (e.g. administration / user rights) shall be put in place to prevent installation of software by all users.

Requests for software installation shall only be accepted where there is a clear business requirement and technical verification.

Anti-malware software will be installed on appropriate points on the network and on server hosts.

4 Backups

4.1 Information Backup

Regular backups of essential business information must be taken to ensure that the Council can recover from a disaster or media failure. An appropriate backup cycle must be used and fully documented by the ICT Service.

Any third parties that store Council information are also required to ensure that the information is backed up securely.

Full back-up documentation, including a complete record of what has been backed up along with the recovery procedure, must be stored at an off-site location in addition to the copy at the main site and must be readily accessible.

All data stored on Council's servers is retained for six weeks after any change or deletion.

Information or data not stored on the Council's servers is not protected by backup procedures and therefore cannot be recovered if amended, deleted or lost.

4.2 Information Restore

Full documentation of the recovery procedure must be created and stored. Regular restores of information must be tested to ensure the reliability of the back-up media and restore process and this should comply with the agreed change management process.

Request to restore deleted or amended data during the six-week retention period should be made through the IT Service Desk.

5 Monitoring

5.1 Audit Logging

Audit logs must be kept for a minimum of six months which record exceptions and other security related events. As a minimum audit logs must contain the following information:

- System identity
- User ID
- Successful/Unsuccessful login
- Successful/Unsuccessful logoff
- Unauthorised application access
- Changes to system configurations
- Use of privileged accounts (e.g. account management, Policy changes, device configuration)

Logs must be protected from unauthorised access that could result in recorded information being altered or deleted. System administrators are not permitted to erase or deactivate logs of their own activity.

5.2 Clock Synchronisation

All computer clocks must be synchronised to the Government Secure Intranet (GSI) time source to ensure the accuracy of all the systems audit logs should they subsequently be needed for incident investigation.

6 Network Management

6.1 Network Controls

Connections to the The Council network infrastructure are made in a controlled and authorised manner. Network management is critical to the provision of Council services and must apply the following controls:

- Operational responsibility for networks should, where possible, be separate from computer operations activities
- There must be clear responsibilities and procedures for the management of remote equipment and users
- Where appropriate, controls must be put in place to protect data passing over the network (e.g. encryption)

The network architecture must be documented and stored with configuration settings of all the hardware and software components that make up the network. All components of the network must be recorded in an asset register.

All devices connected to the Council's network must be security hardened to an appropriate level. Operating systems will have their network services reviewed, and those services that are not required will be disabled.

6.2 Wireless Networks

Wireless networks must apply controls to protect data passing over the network and prevent unauthorised access. Current NCSC encryption standards must be used on the network to prevent information being intercepted

7 Annual Health Check

An independent ICT health check of all Council IT infrastructure systems and facilities must be undertaken by the ICT Service every 12 months. This health check must include, but is not restricted to, the following:

- Penetration test
- A network summary that will identify all IP addressable devices
- Network analysis including exploitable switches, gateways and wireless access points
- Vulnerability analysis, including patch levels, poor passwords and services used

- Exploitation analysis
- A summary report with recommendations for improvement

The IT Health check must comply with the Public Services Network (PSN) code of connection, the Payment Card Industry Data Security Standards (PCI-DSS) and the Cyber Essentials Plus accreditation scheme

As part of the Council's ongoing compliance with the Public Services Network (PSN) Code of Connection, an annual independent IT Health Check by a CREST / CHECK approved vendor will also be undertaken for all systems that have access to a PSN resource.

APPENDIX 4**ICT Remote Working****I User Responsibility**

It is the user's responsibility to ensure that the following points are adhered to at all times:

- Users must take due care and attention of portable computer devices when moving between home and another business site or between business sites.
- Users must ensure that portable computer devices are protected against loss, damage or theft and therefore must not leave them unattended unless the device is secured.
- Users will not change the configuration of any Council-owned portable computer device.
- Users will not install any hardware on a Council-owned portable computer device, unless authorised by the ICT Service.
- Users will allow the installation and maintenance of installed Anti-Virus / Malware and all ICT managed updates immediately.
- Users will inform the IT Service Desk of any Council owned portable computer device message relating to configuration changes.
- All end user devices must be encrypted by the Council and password protected.
- Business critical data must be stored on a Council file server as information stored on portable devices is not included in any backup procedures.
- All faults must be reported to the IT Service Desk.
- Users must not remove or deface any asset registration or serial number.
- No family members may use Council ICT equipment. The ICT equipment is supplied for use by Council officers only.
- The user must ensure that reasonable care is taken of the ICT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, the Council reserves the right to recover the costs of repair.
- The user should seek advice from the ICT Service before taking any Council supplied ICT equipment outside the United Kingdom.
- The Council may at any time, and without notice, request a software and hardware audit. This may require the removal of any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

2 Remote and Mobile Working Arrangements

Users should be aware of the potential of physical security dangers and risks associated with working in any remote office or mobile working location.

Equipment should not be left where it would attract the interests of an opportunist thief. In the home it should also be located out of sight of the casual visitor. Equipment must be secured whenever it is not in use.

3 Access Controls

All computer devices must be switched off, logged off, or have the operating system locked when left unattended, even if only for a few minutes.

All data on portable computer devices must be encrypted.

4 End User Device Updates

Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least every 14 days (or connected via the Council's AnyConnect VPN solution) to enable up to date group Policy and security settings to be applied.

APPENDIX 5**ICT Software****I Software Acquisition**

All software acquired by the Council must be purchased through the departmental IT Business Analyst or a member of the ICT Service. Software acquisition channels are restricted to ensure that the Council has a complete record of all software that has been purchased for The Council computers and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

Personal or unauthorised software (including screen savers, games and wallpapers etc.) must not be loaded onto a Council machine as there is a serious risk of introducing a virus.

2 Software Registration

The Council uses software in all aspects of its business to support the work carried out by its employees. All software is required to have a licence and the Council will not condone the use of any software that does not have a current licence.

Software must be registered in the name of the Council and the department in which it will be used. Due to personnel turnover, software should not be registered in the name of an individual user.

The IT Service Desk and the IT Business Analysts maintain a register of all the Council software assets. The register must contain:

- The title and publisher of the software
- The date and source of the software acquisition
- The location of each installation as well as the serial number of the hardware on which each copy of the software is installed
- existence and location of back-up copies
- The software product's serial number
- Details and duration of support arrangements for software upgrades

Software used on multiple devices shall only be used in accordance with the licence agreement.

The Council holds licences for the use of a variety of software products on all Council information systems and computer equipment. This software is owned by the software company and the copying of such software is an offence under the Copyright, Designs and Patents Act 1988, unless authorised by the software manufacturer.

3 Software Installation

Software must only be installed by the IT Service Desk once the registration requirements have been met. At the time of installation, the appropriate software licences must be verified by the asset owner and ICT Service to ensure that only licensed software is installed.

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may install any free or evaluation software on the Council's systems without prior approval from the IT Service Desk.

4 Software Development

All software and systems developed for the Council are to be used only for the purposes of the Council unless explicit permission is granted by the ICT Service.

Software must not be changed or altered by any user.

5 End User Devices

Council computers are Council-owned assets and must be kept both software legal and virus free. Only software acquired through the procedures outlined above may be used on The Council machines. Users are not permitted to install any software on The Council devices. Council-owned software cannot be taken home and loaded on a user's home devices.

6 Software Misuse

It is the responsibility of all Council staff to report any known software misuse to the IT Service Desk.

Under the Copyright, Designs and Patents Act 1988, illegal reproduction of software is subject to civil damages and criminal penalties. Any Council user who makes, acquires, or uses unauthorised copies of software will be disciplined as appropriate under the circumstances. The Council does not condone the illegal duplication of software and will not tolerate it.