Nottingham City Council

Nottingham City Council

IT Services

Information Security Policy

Safer, cleaner, ambitious
Nottingham
A city we're all proud of

Nottingham
City Council

Reference	**:**	Information Security Policy
Issue No.	**:**	0.1 Draft
Issue Date	**:**	

BUSINESS APPROVAL			
Approved by	**Position**	**Signed**	**Date**
Simon Salmon	**Head of IT Security & Strategy**		

Version History

Version	**Status**	**Author**	**Reason for Issue**	**Date**
0.1	Draft	Liadi Balogun	Interim Policy	10/10/2010
0.2	Draft	Liadi Balogun	Minor amendments	20/10/2010
Final	Draft	Liadi Balogun	GCSx addition	30/10/2010

Distribution List

Copy	**Role**	**Method of Issue**
1.	All staffs	Intranet
2.		
3.		
4.		
5.		

Notes: 1. All roles listed above receive copies, or are notified, of updated versions of the document.
2. The Method of Issue includes provision of paper or electronic copy of authorised document, or notification by e-mail to those with access to the authorised version on the Intranet.

Section 1. Policy

1.1 The ICT Security Policy

Information security management has four basic components:

- Confidentiality: protecting sensitive information from unauthorised disclosure.

- Integrity: safeguarding the accuracy and completeness of information and computer software.

- Availability: ensuring that information and vital services are available to users when required.

Risk Management: Correct assessment of the risks of handling data

Information takes several forms - it is stored on computers, transmitted across networks, held on paper, removable media and conversations. For security purposes, all forms of information must be protected. As such, ICT systems can be the target of many serious threats including computer based fraud, sabotage, vandalism, theft, virus attack, fire combustion and its consequences, user negligence, and computer hacking.

The increased legislative requirements placed upon the Council and the growth of distributed networks throughout the Council present new opportunities for unauthorised access to computer systems. When coupled with the increase of computing away from central mainframe and specialist controls of ICT facilities maintained by the ICT Service (herein referred to as ICT) there is a greater need for service areas, members and employees to take more responsibility for security matters.

The Chief Executive and the Management Team are committed to ensuring that effective ICT Security Management Controls are in place across the organisation at all times. The controls will be set at an appropriate level taking into account the organisation's risk profile, its obligations to comply with regulatory and legal requirements and best practice, also to the need to meet the expectations of the public and all of the Council's other stakeholders. This will be achieved through this ICT Security Policy.

The ICT Security Policy ensures business continuity and minimises business damage by preventing and diminishing the impact of security incidents. The policy enables information to be shared, but ensures the protection of that information and related ICT assets. The nominated officer for Information Security matters within the Council is the Head of IT Security and Strategy (herein referred to as the security manager) who is ultimately responsible for identifying and mitigating security risks to the Council as a whole. However, as further explained in Section 2 (ICT Security Organisation) many other staff also has important responsibilities to discharge under this policy set, and everyone impacted by these policies is required to understand their role in ensuring compliance.

It is the Information Security Policy to ensure that:

- Information security is considered a fundamental, integral part of all of the Council's operations.
- All breaches of information security, actual or suspected, are reported, investigated, documented and acted upon
- Accuracy, completeness and segregation of client data is assured
- Integrity of client data is maintained and protected from attack
- Client data is protected from unauthorised access by employees or other clients of the Council, or third parties
- That where client data is accessed by employees or other clients of the Council or third parties that access to this information is required
- Access is only in accordance with the policy
- Confidentiality of client data from unauthorised disclosure is assured
- Business continuity plans are implemented to support business needs
- Appropriate information security training is given to staff
- Regulatory and legislative requirements are met

1.2. How the Policy is set out

The ICT Security Policy is divided into sections that provide a set of controls based on current security measures in use throughout the Council and supported by ICT, along with industry recognised security protocols.

There are a number of supporting policies that are referenced from the main Information Security Policy. These are:

- Information Security Incident Management Policy
- Information Classification Policy
- Information Backup Policy
- Acceptable Use of Assets Policy

- Remote Home Working policy
- Access Control Policy
- Data Protection Policy
- Removable Media Policy
- Physical Security Policy
- HR Security Policy

1.3. Controls applicable

Some controls are not applicable to every ICT environment and should be used selectively. However, a decision about non applicability may only be made by the Security manager and the default position (in the absence of an explicit statement of exception by the Security manager) is that all controls apply to all environments.

As specified above most of these controls are in use by ICT in their ‘day-to-day’ technical support to the Council’s computer system users and are accepted as "good practice" subject to limiting factors such as legislative, environmental and technological constraints.

1.4 Application of the policy

The policy applies to:

- All employees and elected members of the Council
- All employees and agents of other organisations who directly or indirectly support or use the Council’s Information Systems
- All temporary or agency staff directly or indirectly employed by the Council
- All users having access of any kind to the Council’s systems, resources and/or networks

This ICT Security Policy is intended to be a living document, which will be updated as and when necessary. Sections and appendices can be added to reflect new or amended procedures and guidelines when determined. The policies and controls documented in the ICT Security Policy will be

supplemented by detailed procedures and standards that will form part of the Council's overall information security management system. These will be published from time to time and made available to on a "need to know" basis by the security manager.
All such procedures and standards published under the auspices of the ICT Security Policy will be deemed to form a part of the ICT Security Policy, and breaches of those procedures and standards will be regarded as breaches of the ICT Security Policy itself.

1.5 Annual Review of Policies

The ICT Security Policy will be reviewed at least annually by the ICT Security Group (see section 2 regarding this body). The purpose of the review will be to ensure that the ICT Security Policy continues to meet the needs of the Council (particularly taking into account any changes to the Council's infrastructure, business processes or risk profile since the last review), and that the right balance is being struck between security, usability and cost. Input into the review process will be obtained from a number of sources including the ICT service, user representatives, corporate heads and service managers.

Section 2. ICT Security Organisation
2.1. Management Information Security Forum

Security is a responsibility of everyone associated with the Council. A high level of involvement by senior officers throughout the Authority is necessary to ensure that there is clear direction and visible management support for the ICT Security Policy, Business Risks and associated Security Initiatives/Strategy.

A forum known as the “ICT Security Group” consisting of representatives from service managers and/or appointed representatives, led by the Head IT Security and Strategy and Technical Projects Manager will meet on a regular basis, at intervals no greater than every six months, to address the following: -

- Allocation of ICT security responsibilities
- Specification, procurement and installation of ICT facilities
- Security of third party access
- Specialised security partner
- Analyse reports to security issues

2.2. Allocation of ICT security responsibilities

The security of an information system is the responsibility of the "owner" of that system. Owners of information systems may delegate their security authority to an individual or group, but they remain ultimately accountable for ensuring that adequate security protection is implemented.
The role of the IT Security and Strategy is to advise, monitor and police this owner responsibility. In order to avoid any misunderstanding about this responsibility, it is essential that the areas for which specific operational service managers and/or groups are responsible be clearly defined by way of an agreed protocol.

2.3. Specification, Procurement and Installation of ICT facilities must be technically approved & authorised

Any new ICT facilities, software or databases must be approved by ICT, the security manager and appropriate operational managers so as to ensure that the installation of equipment is for a clear business purpose, will provide an adequate level of physical security protection and will not adversely affect the security of any of the Council's existing business infrastructure.

Business approval - Each installation must have both ICT and the operational service manager's approval authorising its purpose and use. Approval must also be sought from the security manager and/or a senior designated security forum officer responsible for the related security environment to ensure that it complies with the relevant security policies and requirements. See Appendix A for a list of these legislative policies.

Technical approval - It is essential that all devices connected to the Council's LANs (Local Area Networks) and WANs (Wide Area Networks) infrastructures are of an approved type and specification, as supported by ICT.

2.4. Security of third party access

Access to the Council's ICT facilities by third party suppliers might present a security risk. Where there is a business need for such access, the security implications must be assessed and suitable control requirements set out. These controls must be agreed and defined in a specific contract with the third party. Arrangements involving third party access to the Authority's ICT facilities must also be based on a formal contract containing (or referring to) the ICT Security Policy and all of the necessary security conditions to ensure compliance. Where it is necessary for a third party organisation to be granted remote access to the Council's ICT infrastructure, this is a decision that must be approved by the Head of IT Security and Strategy. Where third parties are accessing RESTRICTED data then they will be asked to sign a non-disclosure agreement.

Prior to authorising the ICT service to establish the remote access, the service manager will ensure that:

- there is a clear business need for the third party access to be granted
- the access method does not represent a significant risk to the Council
- there is a written agreement in place with the third party to control and manage the access
- Where possible the access is time constrained
- Access by third parties is reviewed

The Head of IT Security and Strategy will monitor the ongoing business need for the third party access, and will ensure that it is terminated as soon as it is no longer required.

2.5 Specialist Security Partner

Given the specialist nature of ICT Security and the requirement of external objective audit, the Head of IT Security and Strategy shall where required involve a specialist external security partner to audit and assess ICT Security at Council, and to advise on and assist in the implementation of improvements to the security regime as appropriate.

The Council shall ensure that its state of security consistently complies with all necessary standards, is managed and implemented in accordance with the ICT Security Policy, and that any security incidents requiring external assistance are dealt with rapidly and competently.

The framework for the activities of the security partner is as follows:

Regular Activities

- Network software vulnerability and AV currency checks
- Penetration test (internal and external)

Ad Hoc Activities

- Advising on security technologies, and assisting (where appropriate) in their implementation and support
- Advising on new threats to the Council's ICT infrastructure
- Specialist training of staff on security issues
- Specialist testing of introduction of new technologies

Section 3. Asset Classification and Control

3.1. Accountability for assets (including system software)

All items of ICT equipment owned or operated by the Council are hardware assets of the Council. All items of software owned or licensed by the Council are software assets of the Council. The contents of all databases, electronic mailboxes, word processing documents, spreadsheets, web pages, data files, configuration files and other information systems created by officers, members and third parties in the course of their duties are information assets of the Council. All hardware assets, software assets and information assets of the Council (collectively referred to as “ICT Assets”) must be accounted for and have a nominated owner.

An inventory will be maintained of hardware and software assets and each asset clearly identified via an approved asset register/licensing database with appropriate controls clearly defined and designated for that purpose. This inventory will be centrally managed by the IT Security and Strategy team service area. It is the responsibility of the Head IT Security and Strategy that the inventory is regularly checked. It is the responsibility of the nominated owner/user to ensure that any changes to configuration, usage or location are approved by ICT prior to commencement. It is the responsibility of each asset owner to ensure that access to the assets for which they are responsible is controlled and managed in accordance with the ICT Security Policy (and in particular section 7).

3.2. Information Classification Policy

There is a separate information classification policy that can be referred to for classification of information assets.

Section 4. Employee responsibilities for ICT Security

4.1. ICT Security in job descriptions

ICT Security must be addressed at the recruitment stage and included in ALL new employee job descriptions, contracts and induction courses. Job descriptions should define ICT security roles and responsibilities where appropriate. This should include any general responsibilities for implementing or maintaining the ICT Security Policy, outside that required by all employees, as well as any specific responsibilities for the protection of particular systems or for the execution of the ICT security processes.

4.2. ICT Security Education & Training

As part of all induction courses the Council's policies on ICT security must be covered and agreed.

4.3. ICT Incident Reporting Policy

This policy describes the policy for reporting and managing security incidents. This is addressed by Information Security Incident Framework.

4.4. Breaches of the ICT Security Policy

Breaches of the ICT Security Policy will be dealt with in accordance with disciplinary process.

Section 5. Physical and Environmental Security
5.1. Secure Areas

ICT facilities supporting critical or sensitive business activities must be housed in secure areas protected from unauthorised access, damage and interference. They must be protected by a defined security perimeter, with appropriate entry controls and security barriers and any specific environmental conditions recommended by the manufacturer/supplier. Where this provision is not available an action plan will be drawn up and implemented to reduce the risk.

5.2. Security of Core Computer Rooms

Locations housing ICT facilities that support business critical activities will require a higher level of physical security protection. The selection and design must take into account the possibility of all risks: fire, flood, explosion, civil unrest, electrical interference and other forms of natural or man made disaster. Access to the core computer rooms shall be restricted. It is acknowledged that on occasions it may be necessary for visitors to access the secure server room temporarily (e.g. technicians from third parties who supply hardware or software to the Council, security auditors, etc.). Visitors to the computer room shall be supervised at all times. Where keypads are used to access core computer rooms, the keycode should be changed at 3 month intervals or when staff transfer or leave that have access via this keycode. Each location should be assessed from a risk point of view and approached independently.

The computer rooms shall contain at least the following environmental control features:

- Air conditioning
- Environmental Monitoring
- Smoke detectors
- Secure power supply system
- Fire suppression system
- Emergency power off switches
- Fire extinguisher
- Un-interruptible Power Supply

Procedures will be developed for the use of these control features and monitored.

5.3. Security of Network Equipment

Where network equipment has to be located outside of core computer rooms, reasonable steps will be taken to ensure the security of the equipment. Locked cabinets should be used and keys stored securely.

5.4. Work Station/PC Computer Security (including laptops)

All work station/PC equipment must be afforded a level of security that is determined by:

Information/data stored on the equipment (from a data loss point of view)

- Replication or replacement risk
- Location and accessibility
- Portability
- Service value
- The hardware asset value

5.5. Security of Equipment off premises

ICT equipment used outside the Authority's premises, for approved business activities (including laptops), is subject to at least an equivalent degree of ICT security protection, as the above work station/PC and/or office equipment security protocols.

Special care must be taken to protect mobile devices (laptops, mobile phones, USB keys, PDAs etc.), due to the relative ease with which these may be stolen. Users of such devices will observe the following rules:

- Never leave them unattended in a public place
- Do not loan mobile devices to friends or family members
- Never leave equipment in a parked car or near a window
- Take reasonable steps to secure equipment away at night if left in the office or home

See also Removable Media Policy.

5.6 Output Media

Output media containing personal data or system details must not be left where unauthorised persons can read them. Sensitive information must be labelled appropriately and only given to people who are authorised to receive it.
Personal and sensitive data should be correctly disposed of (e.g. blue confidential waste sacks, shredding, and incineration). The principles of the Data Protection Act will be followed when managing output media.
Destruction of personal data should be carried out in a secure manner to provide assurance that it cannot be retrieved by some unauthorised person following deletion or disposal.

Section 6. Computer and network management

6.1. Documented operating procedures

Operating procedures and detailed instructions must be in place for all operational computer systems, to ensure their correct and secure operation. Documented procedures are also required for any systems development, maintenance and testing, especially where it involves cross-functional activities with other groups.

As a minimum, system documentation should include the following:

- Start up and close down procedures
- Inter dependencies with other parts of the ICT infrastructure
- Support contacts
- Back up procedures
- System recovery procedures
- Relevant operating procedures
- Admin username and access

6.2. Segregation of duties

In order to reduce the opportunity for unauthorised modification or misuse of data, where possible the same staff should not carry out the following functions:

- ICT Administrators
- System Administration
- Database Administration
- System Users

Where possible, the authorisation, performance and subsequent checking of a particular activity should be performed by different personnel (although it is accepted that this can give rise to practical difficulties in some situations – however these need to be formally recognised). Managers should be alert to the issue of segregation of duties and use reasonable endeavours to ensure that different personnel are involved in different phases of particular activities that could be used to perpetrate fraud or undermine the Council’s security regime. It is recognised that due to capacity issue this segregation of duties cannot always be carried out. Other risk controls should be implemented in these situations.

6.3. External contractor management

The use of external contractors/companies to manage application and system software introduces a number of potential security exposures - such as compromise, damage, or loss of data. These risks must be identified in advance and appropriate measures agreed with the contractor and incorporated within their contract of employment/engagement. These measures must be no less stringent than those applied "in-house".

6.4. Operational change control

The Council has formal change control management responsibilities and procedures in place to ensure satisfactory control of all changes to equipment, software and procedures.

6.5. Protection from malicious software (Virus Controls)

It is essential to ensure that the Council network remains virus free, and that any penetration by any virus (or other malicious software) is immediately detected and the threat is contained and dealt with before any damage can occur. This is achieved through a multi tiered approach to the threat:

- Ensuring current anti virus software is always in place right across all Council Information Technology Assets
- Ensuring that all users of Council Information Technology Assets follow straightforward procedures to reduce the risk of viruses accidentally being let in to the organisation
- Ensuring that the vulnerabilities that viruses generally exploit are not present anywhere on the Council network
- Ensuring that appropriate processes are in place to minimise loss and deal effectively with viruses that are detected

Council approved standard anti-virus software shall be installed on all of Council's servers, workstations, personal computers, laptops and notebooks, and automatic scanning for viruses shall be activated whenever such equipment is in use. Irrespective of medium, (for example: CDs, USB keys and/or email attachments) the input of any software or data into the Council network shall pass through the Council's anti-virus controls so as to minimise the risk of viruses entering the Council network.

If a virus does enter the Council network then this shall be dealt with effectively and promptly by ICT so as to minimise risk to the organisation. This might include a complete machine rebuild.

Additionally, all users of Council Information Technology Assets have a personal responsibility to play their part in protecting the Council network against malicious software.

In particular, users are responsible for ensuring that:

- They do not inadvertently introduce a virus from an external source into the Council network
- When using Council Information Technology Assets, the equipment that they are using is running anti-virus software with up to date file definitions
- The use of output media (see Appendix B) is particularly susceptible to virus and as such ICT should be informed when any such media is used that may have been used outside of the authorities network.
- They report any suspicious incidents immediately by (in the first instance) contacting the ICT Helpdesk
- They follow any instructions received from the ICT service regarding dealing with a virus threat.

6.6. Vulnerability and Patch Management

The ICT services are responsible for keeping abreast of identifications of new vulnerabilities that could impact Council Information Technology Assets and for implementing patches accordingly. Where possible, software will be used to automatically deploy updates to Council Information Technology Assets. Where automatic systems are not available periodic checks will be conducted to ensure that new vulnerability threats are identified and dealt with in a timely manner. Where the responsible individuals make a determination that there is a potential impact associated with a new vulnerability they shall immediately contact the ICT Manager and determine an action plan.

The action plan will typically comprise:

- Risk assessment and testing
- Implication for other ICT infrastructure
- (If required) further research and verification with a trusted external information security advisor who is familiar with the Council network
- Implement a patch on all Information Technology Assets potentially impacted by the vulnerability.

Patch implementation shall be conducted taking into account the need to minimize system downtime whilst still ensuring implementation of patches to all potentially impacted machines in a timely manner.

6.7. Data backup Policy

The Data backup policy describes in more detail the provision of data backup. This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of equipment failure, intentional destruction, accidental loss or disaster.

6.8. Specification of Communications Networking Standards

In order to maintain acceptable levels of wide and local area network integrity and performance it will be necessary for all system elements to be of a standard approved by ICT, in line with the ICT Strategy.
Total responsibility lies with ICT for any network installations planned to connect with the corporate network.
Secure configuration of the infrastructure is critical to Council's information security regime. Configuration practices should reflect the need for security to be set at an appropriate level given the Council's risk profile, regulatory and legal requirements and user needs. Security practices must also strike a balance between reducing risk and allowing business processes to function.

Configuration shall reflect the following core security principles:

- Defence in depth: Systems should be configured securely to level of best practice

- Security as a Priority: The security of the system will be not be compromised as a principle
- Principle of least privilege: Users and systems should only be given as much access as they need to do the job
- A system is only as secure as the weakest link.
- Consideration if the information should not be available over the computer network

The Council's ICT infrastructure will be segmented such that there are clear divisions between the internal network and the other unknown and or external traffic. A firewall shall separate the internal network from the zones carrying unknown traffic.

6.10. Disposal of hardware

When a hardware asset is decommissioned, the ICT service shall ensure that all information stored on decommissioned hardware and output media is irretrievably destroyed, in order to protect the confidentiality of the data they contain. This may mean physical destruction or low level reformatting of hard drives; the precise mechanism will be dictated by the nature of the device being decommissioned but using best practice (e.g. number of overwrites).

6.11 Monitoring and Logging

Logging involves the collection of event data on devices within the ICT infrastructure. Logging processes also encompass the analysis of logging data, the alerting of the ICT service to unusual and suspicious activity, and appropriate storage of log files.

As well as alerting the ICT service to suspicious activity within the ICT infrastructure, logs provide an audit function that allows the ICT service to review compliance with security policies (e.g. access control). The Council's logging process will cover the following components of the ICT infrastructure:

- Internal servers
- Network devices including Firewalls and Routers

Logging processes will be managed at an individual device level in order to ensure that they are not overwritten and are kept to a manageable size.

- Log files must be automatically rotated so that files are not overwritten
- Log files must be kept locally for a minimum of 90 days
- Log files entries must be time stamped

All Windows event logs and UNIX style syslogs generated are to be collected in a centralised location and stored on a secure server. Logs collected on the centralised system should be kept for a minimum of 6 months.

The logs on the centralised server are to be monitored for anomalous events using appropriate software tools. Anomalous activity includes, but is not restricted to the following events:

- Port-scan attacks or repeated login attempts
- Access policy violations
- Suspicious traffic activity, for example large number of connection events to a web server
- Failed file and object access attempts

In addition, logs should be monitored for 'normal' activity of a significant nature.

Examples include:

- Changes to system security configuration
- System shutdowns and restarts
- Privileged operations
- Access to files classified as Secret
- User and group changes in Active Directory

Log entries should be categorised in order to determine the severity of the event, and to aid filtering and auditing of log files. At a minimum the categories should include Informational, Warning and Error. Logs will be reviewed on a regular basis for

- Unusual or anomalous events
- Events that have a 'serious' categorisation - e.g. errors or critical events
- Violation of security principals such as segregation of duty and least privilege
- Violations of the Access Controls policy

An alerting mechanism shall be in place for serious security events:

- The alerting system shall notify a designated ICT service member by email, sms and /or pager
- Notification should happen within 30 minutes of the event
- The ICT department member designated to receive alerts should be on call and be able to take action on security incidents at any time, including weekends, out of normal business hours and holidays
- When an alert is received, the procedures set out in ICT Incident Policy shall be followed.

Section 7. System Access Controls
7.1. Documented Access Control policy

The Council is committed to implementing and maintaining strong access controls to prevent unauthorised access to its systems and data, whilst simultaneously ensuring that all users have levels of access consistent with their needs in order to carry out their duties efficiently.
An Access Control Policy has been created and is a supporting document to the IT Security Policy.

7.2 Employees/Officers and Members rights of Inspection of data/documents

The Council has strict rules, in-line with both legislative and Council policies, governing the access to documents by its employees and members. These rules apply just as much to those held in electronic form as they do for those held in paper form.
Council employees and members are also governed by the Data Protection Act legislation. Full details are in the data protection policy.

Section 8. System Development and Maintenance
8.1. Security Requirements, Analysis and Specification

The Head of IT Security and Strategy is required to analyse the security requirements of all systems at the time the system specification/business case are made. These must also be considered when evaluating software packages and when any configuration changes are made.

8.2. Information Records Requirement

When specifying, implementing or reconfiguring systems it is important to take into account the Council's information records management policies.

8.3. Controls of Operational systems/software

In order to minimise the corruption of information systems, strict controls are necessary over the implementation of any changes. Change control procedures must be in place to ensure that security and control procedures are not compromised. In all such cases appropriate agreements/approvals, along with correct procedural approaches must be granted before any changes can be implemented that may impact on other business critical systems. When an operational service system needs to be closed down during normal office hours a proper impact assessment needs to take place and agreement made with key stakeholders.

8.4. Review of Operating System changes

It is often necessary to change operating systems (e.g. new release, software upgrade etc.). Before changes are made, the necessary checks must be made to ensure that there is no adverse impact on security.

8.5. Restrictions on changes to software packages

Where modification to software packages is essential an impact assessment, at an appropriate management level, must be made to ensure that there is no adverse impact on security. Version control and a record of all patches applied will be maintained and appropriate licenses have been logged and granted. In addition full documentation should be supplied.

Section 9. Business Continuity Planning

9.1 Business Continuity

Inevitably services may fail on occasions and the duty for the Council/ICT is to resume business continuity immediately, whilst reviewing the reasons for this failure of service and making appropriate changes where necessary. Business Continuity (BC) planning involves identifying and reducing the risks from deliberate or accidental threats to all the Council's vital services. ICT currently have appropriate disaster recovery (DR)/BC procedures and plans developed to enable ICT operations to be maintained following failure or damage of vital services or facilities.

The procedures and plans will be tested and reviewed on an ongoing basis. The Council's Business Continuity procedure describes in more detail the process and procedures that are in place.

Section 10. Compliance and Audit

10.1. Controls of proprietary software copying (Licensing)

Proprietary software products are usually supplied under a licence agreement that limits the use of the product to a specified or a number of specified machines or users and may limit the copying to that of source back up copies only. Copyright infringements can lead to legal action and criminal proceedings against the Council and individual employees/Members concerned. It is the Council's policy in-line with the ICT Security Policy to ensure compliance with all legal obligations and to further ensure that no copyright material is copied without the owner's consent.

The Head IT Security and Strategy is responsible for all such copyright material and monitors, controls, and further maintains a register/database of all copyrighted licenses accordingly. A regular audit is performed by the service manager of this database

It is the responsibility of the Head IT Security and Strategy r and designated ICT personnel, along with employee responsibilities to ensure that this software license inventory is regularly checked. It is the responsibility of the owners (heads of service areas or delegated security officers) of the ICT equipment on which the software is running to ensure that appropriate licences are registered on the ICT asset register/database.

10.2. Safeguarding the Council's records

Some records are needed to meet statutory requirements and must be securely retained. It is however appropriate to destroy records that have been retained beyond the statutory retention time, in a secure manner in line with the ICT Security Policy and adopted procedures there-in.

10.3. Data Protection Legislation

Personal information on living individuals who can be identified from information that is stored in any format is subject to The Data Protection Act 1998. The Council's Data Protection Policy should be used for further information. The ICT Security Policy Access fully supports the Data Protection Act and will ensure that IT systems used to store personal and sensitive data are on a need to know basis, authorised by service manager to ensure lawful processing of personal data. There will be specific training for ICT staff and to raise the awareness of the implications of the Data Protection Act. Destruction of personal data will be carried out in a secure manner to provide assurance that it cannot be retrieved by some unauthorised person following deletion or disposal.

It is the responsibility of the owner of the data to notify the Data Protection Officer of any proposals to keep personal information on a computer and/or a paper based system and to ensure compliance with the principles laid down in the legislation.

The Head IT Security and Strategy will also advise on the ICT Security considerations as laid down by the Act.

For further information please refer to the Head IT Security and Strategy or the Data Protection Officer.

10.4. Prevention of misuse of ICT facilities

All of the Council's ICT facilities are provided primarily for business purposes only and covered in the acceptable use policy.

10.5. Compliance with the ICT Security Policy

Owners of all Council information must hold regular reviews of the compliance of their systems in order to meet the Council's ICT Security Policy, Standards and other security legislative and non-legislative requirements.

10.6. System Audit Controls

ICT Security and Audit requirements/activities involving checks etc. on Council operational systems must be carefully planned and agreed to minimise the risk of disruption to normal business working practices.

10.7. Protection of System Audit tools

Any ICT Security and Audit tools, Computer Assisted Audit Techniques software and/or data etc., must be safeguarded to prevent any possible misuse or compromise.

Section 11. Infrastructure Management

11.1. Security Hardening

All ICT infrastructures, to include servers and workstations, will be approached from a view of security hardening using best practice.
The will include:

- Ensuring that only the required services are running on the machine
- Software is up to date and patches have been applied
- Anti-virus is up to date and centrally managed
- Where possible personal firewalls will be enabled
- Only the applications that a user requires is installed for use
- Local accounts not required are removed where possible

11.2. Patch Management

A patch management scheme has been developed to ensure that proper patch management is carried out on the ICT infrastructure. This will take a risk management approach to ensure that patches are applied as soon as possible whilst balancing this with risks if the patch installation process fails. This patch management scheme will include incremental patches as well as cumulative service packs.
Supplier's web sites will be pro-actively monitored, and where possible email alerts used or other automatic systems, to ensure that patches are made available to install as soon as possible. Access to GovCertUK and the East Midlands WARP security alerts will be used as part of the risk management approach.

11.4. Software out of support and maintenance

Where software has been identified as being out of support and maintenance and therefore not providing any patches an action plan should be created to manage this situation using a risk management approach. All software should be procured on the basis that it can be supported and upgraded to ensure that all security risks are minimised.

11.5. Ports

A list of ports that are used should be created on a per application basis. Personal firewalls will be configured to only allow these defined ports to be opened for the applications on an individual machine.

11.6. Administrator Privileges

Users should not be using administrative privileges to carry out their normal work activities. Where administrative privileges are required to run applications the supplier of the software will be contacted and a resolution sought to allow the application to run as a non-administrator and a risk management action plan implemented to improve the situation. Where an application is identified as requiring administrative privileges other applications, especially web browsers and email clients, should still be set to run as non-administrative users.

Section 12. The Council's Disciplinary Process
12.1. Disciplinary Process

In all cases breaches of the ICT Security Policy will be dealt with in accordance with the Council's disciplinary procedures process. This process is a deterrent to employees who might be inclined to disregard the ICT security procedures covered by this policy and ensures a correct and fair treatment for those who are suspected of committing serious or persistent breaches of ICT security. Members are also responsible within this document for their breached of the ICT Security Policy and a standards process exists that would allow a serious breach to be escalated.
For further information please refer to the Council's disciplinary processes and procedures.

Section 13. Access to the GCSx Network
13.1. Government Connect Secure Extranet (GCSx)

The Government Connect Secure Extranet (GCSx) is the network used to access the DWP systems and in particular access to the Customer Information System (CIS).
In order to maintain this access a number of security measures will be required. The Council is fully committed to achieving and maintaining the compliance required to connect to the Government Connect Secure Extranet (GCSx). The Memorandum of Understanding between the Department for Work and Pensions (DWP) and the Council sets out the framework and operating policy through which the Council will access benefits data for the administration of Housing Benefit and Council Tax Benefit. This data will be available via DWP's Customer Information System. It will include access to DWP benefits data and Her Majesty's Revenue and Customs' tax credit data. In order to access the Government Connects the compliance is measured through a formal document called the Code of Connection (CoCo). The GCSx is the network used to access the DWP systems.

13.2 GCSx – Restricted Data

The Council is defining RESTRICTED information is where either information that:

- links an identifiable individual with information that, if released, would put them at significant risk of harm or distress or
- Any source of information relating to 1000 or more individuals that is not in the public domain, even if the information is not likely to cause harm or distress

For the purposes of the Code of Connection the scope of RESTRICTED is limited to the Housing Benefit and Council Tax Benefit system. This scope will be reviewed in accordance with any change of use to the GCSx.

13.3. Management of Users

The Council will maintain a list of all users that will have access to the GCSx. These users will have specific requirements that must be met:

- Each user must be allocated a unique user name to logon to their machine and to log on to CIS.
- All users of the must meet the following password complexity
    1. minimum of seven characters;
    2. alpha-numeric and contain at least 1 digit;
    3. changed a minimum of every 90 days; and
    4. not reused within 20 password changes

13.4. Baseline Personnel Security Standard

Each user of the network connected to GCSX who has regular access to RESTRICTED information or information that originates from the GSi must be at least cleared to the 'Baseline Personnel Security Standard' (BPSS).
This includes

- Proof of Identity,
- Nationality,
- Employment History,
- Requirement to disclose any unspent convictions

13.5 Access to RESTRICTED systems for remote users

Access for users using remote methods to connect to systems with RESTRICTED data is specifically prohibited unless this has been approved by the Head of IT Security and Strategy.
Remote methods this includes access from home machines, access from laptops used on external networks and any other access from outside of the current network. Access from outside the United Kingdom is, by definition, specifically prohibited.
Where access is provided on an agreed basis then two-factor authentication methods will be used. This also applies to ICT Staff who may have access to remotely manage and monitor systems.
Where third parties are accessing RESTRICTED data then they will be asked to sign a non-disclosure agreement.

13.6 Personal Commitment Statement

All users of the GCSx network will be required to sign a personal commitment statement. This commitment statement ensures that each individual user is aware of the risks of using the network and their responsibilities.

The IT Security Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.
The current version of this document is available to all members of staff on the corporate intranet.