City of Lincoln Council

Information Security Policy

CONTENTS

Roles within the Policy

Council	**City of Lincoln Council**
Corporate Management Team	**Corporate Management Team**
Head of IT	**Assistant Director – Strategic Development**
IT Security Officer	**Business Development and IT Manager**
IT Manager	**Business Development and IT Manager**
IT Security Group	**ICT and Information Governance Board (AD Group)**
IT Department	**Business Development and IT Team**
IT Helpdesk	**IT Helpdesk**
Human Resources	**Human Resources and Work Based Learning Manager**
Data Protection Officer	**City Solicitor**
Property (Physical Security)	**Chief Finance Officer**

Section 1 - Introduction

The purpose of this document is to set out the Information Security Policy for City of Lincoln Council ("the Council"). It demonstrates management commitment to having in place sound information security arrangements, gives clear direction to managers and staff, and will ensure that legal requirements and best practice standards are met.

It is not intended to be exhaustive guidance and therefore should be read in conjunction with other Information Governance Policies and supplementary guidance which will be updated periodically by the Business Development and IT Team. These documents include guidance on:

Policies

- Data Protection Policy
- Freedom of Information Policy
- Information Governance Policy
- Information Sharing Policy
- Records Management Policy
- Legal Responsibilities Policy
- Data Protection Breach Management Policy
- Data Quality Policy

Supplementary Guidance

- Acceptable Usage
- Bring your Own Device (BYOD)
- Communications and Operations Management
- Computer, Telephone and Desk Use
- Email
- Human Resources Information Security Standards
- ICT Project Management Guidance
- Incident Management
- Information Classification
- Information Protection
- Internet Acceptable Usage
- IT Access
- IT Infrastructure Security
- Payment Card Industry Data Security Standard (PCIDSS)
- Remote Working
- Removable Media
- Software

Other Information

- Risk Management and Accreditation Document Set (RMADS)

Section 2 - Policy

2.1 The Information Security Policy

'City of Lincoln Council will seek to ensure that the Confidentiality, Integrity and Availability of its information is maintained at all times'

Information security management has three 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.***

Information takes several forms - it is stored on computers, transmitted across networks, held on paper, microfiche, tapes, disks, removable storage devices, computers and conversations. For security purposes, all forms of information must be protected. As such, IT systems can be the target of many serious threats including: *computer based fraud, sabotage, vandalism, theft, virus attack, user negligence, disaffected employees, third party support organisations and computer hacking.*

The growth of distributed networks throughout the Council, presents new opportunities for unauthorised access to computer systems. When coupled with the increase of the increased legal and externally imposed responsibilities, there is a greater need for departments/employees to take more responsibility for security matters. It is the responsibility of each employee to adhere to this policy.

The Chief Executive and the Corporate Management Team are committed to ensuring that effective IT 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 e.g. as shown in appendix A, and the need to meet the expectations of the public and all of Council's other stakeholders. This will be achieved through this Information Security Policy. Furthermore the Information 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 IT assets.

The nominated officers for Information Security matters within the Council are:

- IT Security – Assistant Director – Strategic Development
- Information Management – City Solicitor
- Physical information security – Chief Financial Officer

who are ultimately responsible for identifying and mitigating security risks to the Council as a whole. However, as further explained in Section 2 (IT Security Organisation) many other staff also have important responsibilities to discharge under this policy set, and everyone impacted by these policies is required to understand what their role is in ensuring compliance.

The following sections provide a set of controls based on current security measures in use throughout the Council and supported by IT, along with industry recognised security protocols.

These are the controls and recommendations on which this policy is based.

2.2 Controls applicable

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

As specified above most of these controls are in use by IT 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.

2.3 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, or who have access to information pertaining to the Council's 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 Information 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 Information Security Policy will be supplemented by detailed procedures and standards that will form part of Council's overall information security management system. These will be published from time to time and made available on a "need to know" basis by the IT Security Officer. This policy and supplementary guidance, where they affect employees' activities will be made available to all employees who will need to accept and operate within the guidance provided. All such procedures and standards published under the auspices of the Information Security Policy will be deemed to form a part of the Information Security Policy, and breaches of those procedures and standards will be regarded as breaches of the Information Security Policy itself.

2.4 Review of Policies

The Information Security Policy will be reviewed at least every two years by the IT Security Group (see section 2 regarding this body). The purpose of the review will be to ensure that the Information 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 IT Department, user representatives, and Assistant Directors. In addition, the IT Security Officer will have commissioned an annual compliance audit by an external information security specialist to identify material aspects of non-compliance (if any) with the Information Security Policy and external compliance requirements.

Section 3 - IT Security Organisation

3.1 Management Information Security Forum

Security is a responsibility of everyone associated with the Council.

3.2 Statement from the Chief Executive

The City of Lincoln Council has a Strategic Priority of providing 'High Performing Services'. A key enabler to achieve this aim is the provision of a reliable and resilient ICT infrastructure, providing services to support officers, and increasingly satisfying customer requirements directly through online services. While ICT can bring major benefits in terms of business process, customer support and improved ways of working there is a responsibility on all of us to operate within a controlled environment in line with best practice standards and legislative requirements.

I, and the Corporate Management Team, take these responsibilities very seriously and by endorsing this document show our commitment to the safe-keeping of information entrusted to us for the delivery of public services.

Within the organisation, everyone has a responsibility for the management of information:

- ***Corporate Responsibility** – to ensure that policies and procedures are in place and resources are allocated to manage and monitor the use of ICT.*
- ***Line Manager Responsibility** – to ensure that policies are communicated to staff, and that such policies are adhered to.*
- ***Individual Responsibility** – to read, sign-off and adhere to the ICT Security Policy.*

I am confident that the policy will be applied diligently by all staff, providing benefits to staff and customers alike.

Angela Andrews
Chief Executive and Town Clerk

3.3 IT Security Group

As well as the IT Security Officer, 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 Information Security Policy.

A forum known as the "IT Security Group" (consisting of the IT Security Officer and departmental system administrators/representatives), but lead by the IT Security Officer will meet on a regular basis to address the following as necessary: -

3.4 Allocation of IT 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 owners of Council’s core information systems are detailed in **Appendix B**.

The IT Security Officer’s responsibility is to advise, monitor and ensure the organisation is operating in accordance with this policy. It is essential that the areas for which the IT Security Officer, specific managers and/or groups are responsible be clearly defined.

3.5 Installation of IT facilities must be technically approved & authorised

Any new IT facilities must be approved by IT, the IT Security Officer and appropriate 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 IT and the Service’s Assistant Director’s approval authorising its purpose and use. Approval must also be sought from the IT Security Officer 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. The initial business case for new installations should include costs and other implications of ensuring compliance with IT Security policies. In addition projects of a strategic nature require approval through the Authority’s Strategic Plan Implementation Team.

Technical approval - It is essential that all devices connected to the Council’s LANs (Local Area Networks) and WANs (Wide Area Networks) infrastructures adhere to government standards and specification, and reflect the relevant Information Classification of the system.

3.6 Security of third party access

Access to the Council’s IT 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. All third party employees must be security checked and verified to a level appropriate to the systems and data being accessed, before being afforded access.

Arrangements involving third party access to the Authority's IT facilities must be based on a formal contract or Service Level Agreement (SLA)) containing (or referring to) the Information Security Policy and all of the necessary security conditions to ensure compliance. Any alterations made to the SLA during the contract period must be formalised through the IT Security Officer and documented accordingly.

Any connection by third party IT (e.g. Laptops) must be authorised by the IT Security Officer

Where it is necessary for a third party organisation to be granted remote access to the Council’s IT infrastructure, this is a decision that must be taken by the IT Security Officer.

Prior to the remote access being authorised, the IT Security Officer will ensure that:

- there is a compelling business need for the third party access to be granted
- there is a written agreement in place with the third party that includes (as a minimum) the following provisions
    - an agreed Code of Connection between partners appropriate to the level and type of access
    - an Information Sharing Agreement where personal or sensitive data is being shared and/or contract for the service being delivered as appropriate.

The IT Security Officer 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.

3.7 Specialist Security Partner

Given the specialist nature of IT Security and the requirement of external objective audit, the IT Security Officer shall on a regular basis involve specialist external security partners to audit and assess IT Security at the Council, and to advise on and assist in the implementation of improvements to the security regime as appropriate.

The IT Security Officer will review the choice of the external security partner annually.

The Council shall use this organisation as a trusted partner to assist in ensuring that its state of security consistently complies with all necessary standards, is managed and implemented in accordance with the Information Security Policy, and that any security incidents requiring external assistance are dealt with rapidly and competently.
The performance of the Security Partner will be governed by a formal contractual arrangement covering definitions of services to be provided and all associated commercial terms.

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

Regular Activities

- Annual auditing of compliance with the Information Security Policy, and recommendations for changes
- Annual internal network software vulnerability and anti-virus currency checks and annual penetration test in line with external compliance requirements e.g. TIGER, CHECK or Crest Accredited.

Ad Hoc Activities

- Assisting in ad hoc resolution of security incidents
- Advising on security technologies, and assisting (where appropriate) in their implementation and support
- Advising on new threats to the Council’s IT infrastructure
- Specialist training (if required) of the Council’s Information Technology Department and other relevant officers.

Section 4 - Asset Classification and Control

4.1 Accountability for Assets (*Including system software*)

All IT equipment owned or operated by the Council are hardware assets of the Council. Personal Electronic Devices are permitted to be used to access some data at the discretion of the IT Security Officer in line with guidance provided by Central Government.

All 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 and are subject to audit at any time.

Any information provided to the Council by other organisations will be managed appropriately, and subject to requirements set out by the providing organisation.

All hardware assets, software assets and information assets of the Council (collectively referred to as “IT Assets”) must be accounted for and have a nominated asset owner.

An inventory will be maintained of all such Council IT assets and each asset clearly identified via an approved asset register/licensing database with appropriate controls clearly defined and designated for that purpose. This will be maintained in accordance with the Council’s Asset Management Policy. An inventory of IT assets is held by the Business Development and IT section. The inventory should include insurance values for the equipment.

It is the responsibility of the IT Manager that the inventory is regularly checked. It is the responsibility of the nominated owner to ensure that any changes to configuration or location of the assets are approved by IT 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 Information Security Policy (and in particular section 7).

4.2 Information Classification Guidelines

The Council is committed to protecting the confidentiality of all of its sensitive information, and also to protecting confidential information belonging to third parties which has come into the possession of Council. In particular, the Council is committed to ensuring compliance with its legal obligations under privacy legislation and arising from confidentiality agreements with business partners.

The person who creates a file or database is responsible for the classification of the data contained within. The classification shall be consistent with the descriptions given below. The default classification is “OFFICIAL”.

All Council information shall be classified according to the Information Security Classification Policy:

All information will be designated as OFFICIAL by default. Where information is considered to require higher levels of control e.g. more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, this may require a higher classification. This information should still be managed within the “OFFICIAL‟ classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the “need to know‟. In such cases where there is a clear and justifiable requirement to reinforce the “need to know‟, assets should be conspicuously marked: ‘OFFICIAL–SENSITIVE’.

A schedule of information that is considered to be OFFICIAL-SENSITIVE will be maintained by the Authority.

4.3 Working with Different Classifications of Information

Different classifications of information need to be protected by applying different controls. These are set out in the Information Security Classifications Policy. It is the responsibility of the person who creates a file or database to ensure that the appropriate protections are implemented.

Systems will be classified at an appropriate level based on the security profile and potential access methods to the system. No information classified above the level of the system shall be stored on the system without authorisation from the IT Security Officer.

Only information relevant to a system shall be processed on that system. Extreme care shall be taken to ensure the protection afforded to a system is appropriate for the level of information being processed.

Owners of information assets shall periodically review samples of data for which they are responsible, and check to ensure that the provisions of this policy document are being properly applied across their area of responsibility.

In order to determine appropriate classification levels owners should refer to relevant the Information Security Classifications Policy or confirm with the SIRO/Information Governance Officer.

4.4 Secure disposal of equipment

The authority currently has an approved Disposal of IT Equipment Policy, which constitutes part of this Information Security Policy. All storage media must be checked to ensure that all data is erased and licensed software has been removed prior to its disposal, and should be disposed of through the IT Team. The classification of the material to be disposed of will govern the method of disposal.

Section 5 - Employee Responsibilities to IT Security

5.1 Security in job descriptions

Security must be addressed at the recruitment stage and included in the code of conduct, employee job descriptions where necessary, contracts and induction courses. Job descriptions should define IT security-related roles and responsibilities, where appropriate, as designated by both the IT Security Officer and the IT Security Group. This should include any general responsibilities for implementing or maintaining the Information Security Policy, as well as any specific responsibilities for the protection of particular systems as laid down in system **Security Operating Procedures (SYOPS),** or for the execution of the IT security processes. Employees with access to systems or information, will sign as understanding their role and responsibilities.

5.2 Security Education & Training

As part of all induction courses information security must be included, and the Council's policies on IT security must be covered. To ensure the integrity of all the Council's data, staff should have received training on any application that they would be required to access/support and any software package they will be required to use, and training records maintained by system owners.

In addition to IT Security, the council also operates a clear desk / clear screen guidance. Therefore, all information must be secured at the end of each working day, computers logged off and computer screens powered off.

5.3 Reporting of and Managing IT Security Incidents

Incidents affecting IT security must be reported through the correct channels as quickly as possible. All employees and contractors must be made aware of the procedure for reporting the different types of incident – IT security breach, threat, weakness or malfunction - that might have an impact on the security of the Council's data or assets. They must also report any observed or suspected incidents as quickly as possible to the IT Security Officer or the IT Helpdesk dependant on the security incident being reported.

Whilst investigation is underway, the IT Security Officer shall give active consideration as to whether the access rights of any individual or group should be temporarily suspended.

Users should act on the basis that if they are in any doubt, a notification should be made. No one will be penalised for raising what subsequently turns out to have been a false alarm (provided, of course, that they were acting in good faith).

Security incidents are defined as any of the following:

- ➢ Any breach of the Council IT Security Policies and Procedures
- ➢ The compromise of any Council information security controls
- ➢ Any use of any Council Information Technology assets that is perceived to be illegal, harassing, offensive or that can adversely affect the integrity and reputation of the Council

- Any attempt, successful or otherwise, to gain unauthorised access to Council information systems resources
- The use of unauthorised Council computing resources for personal gain
- Refusal to co-operate with any reasonable security investigation
- Unauthorised access, viewing, disclosure or manipulation of confidential data, information, applications, systems or any other Council information systems resources
- Using the assistance of or soliciting a third party to circumvent the Council's information security controls.

The IT Helpdesk shall ensure that the person who reported the incident is responded to. If that person is not satisfied that the incident is being investigated appropriately, then they shall contact the IT Security Officer.

The response to a security incident by the IT Department must cover the following steps in the sequence set out below:

- Notify the IT Manager
- Prevent the spread (or "propagation") of the problem
- Ensure that any forensic evidence of the incident is captured and retained for subsequent investigation (this may include physical evidence or log files for example). The IT Security Officer is responsible for capturing such evidence, and will be trained appropriately.
- Restore normal service
- Investigate the cause of the problem, and resolve
- Implement any changes to the information infrastructure necessary to solve the problem that caused the incident
- Ensure communication to all appropriate parties of what occurred, how it was dealt with and what lessons should be learned
- Report in accordance with the Council's incident reporting system where equipment or data has been lost or stolen.

All incidents are to be logged and recorded for future reference, training needs as appropriate, lessons learnt and mitigation of future risk.

5.4 Breaches of the Information Security Policy

Breaches of the Information Security Policy will be dealt with in accordance with Section 12 Disciplinary Process.

5.5 Termination of Employee Access

Immediately following termination of an employee's requirement for access or of a third party assignment, their access rights shall be revoked in accordance with the procedures set out in section 7.

It is the responsibility of the employee or the third parties line manager to liaise with HR and the IT Department to ensure that the access termination provisions are executed.

Further information can be found in the Authority’s Disciplinary procedures.

5.6 General

When a member of staff leaves the employment of the Council, changes duties or their access requirements change, it is the responsibility of their manager to ensure that all building access cards, manuals, ID cards, IT equipment, mobile phones, etc, are returned on or before the day of leaving. Managers are also responsible for reviewing their staff’s access requirements on a regular basis.

Section 6 - Physical and Environmental Security

6.1 Secure Areas

IT 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.

6.2 Security of Server rooms

Locations housing IT 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 manmade disaster. Further information can be found in the Authority's BCP/DR Plans

Keyed access to the server room shall be restricted to the IT Team. A spare key is available and secured by the Council's Property Assistant and the Manager, Property Services. When not in use, the access points to these facilities are to be secured and strict access control exercised.

The IT Department's offices are to be keyed on a separate key system from the rest of the building.

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 server room shall be supervised appropriately and must sign in, in accordance with the council's policy on visitors.

In order to adequately protect the server room and the equipment contained therein, the following activities are strictly prohibited within the server room at any time:

- Smoking
- Drinking
- Eating
- Littering
- Other inappropriate behaviour

The server room shall contain the following environmental control features:

- Air conditioning
- Raised platform for servers
- Smoke detectors
- Secure power supply system
- Fire suppression system
- Emergency power off switches

- Fire extinguisher
- Key Locks
- Un-interruptible Power Supply
- Humidity Control

No employee shall tamper with or do anything that could interfere with the proper operation of any of the control features listed above.

All environmental controls will be subject to periodic inspection/testing and maintained as required.

6.3 Work Station/PC Computer Security (including laptops)

All Work Station/PC equipment must be afforded a level of security that is determined by its asset, information content or service value. Various controls are available from suppliers that will physically protect equipment from opportunist to calculated theft.

IT must hold the configuration details of all related Work Stations/PC's.

6.4 Security of Equipment off premises

IT equipment used outside the authorities premises for approved business activities (including laptops), is subject to at least an equivalent degree of IT security protection, as the above Work Station/PC and/or office equipment security protocols. In particular the Council's mobile working protocol must be adhered to. Any data which is held on mobile devices should be encrypted to appropriate standards.

Special care must be taken to protect mobile devices (laptops, mobile phones, USB keys, PDAs etc.), due to the relative ease with which these items 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 them in a parked car or near a window
- Do not check them in as baggage when flying
- Consult travel guidance before taking them to other countries

6.5 Electrical Supplies

Information stored on computers can be lost or damaged if a power surge or power cut occurs. Where critical systems are concerned, they should be fitted with equipment that will protect against this and other power problems. Business continuity and Disaster Recovery plans should be in place should equipment be compromised in this manner.

6.6 Physical and Electronic Media

Media containing personal data or system details must not be left where unauthorised personnel can read them. If possible, when not in use, they should be kept in a locked cupboard. 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. shredding, incineration) according to the classification of the information.

Only approved Council-owned IT-provided media should be used and media must be encrypted.

6.7 Homeworking and Remote Working

It will be necessary for business reasons for some staff to work from home or other remote locations. In order to maintain levels of security, the homeworking and remote working policies, available from HR and BDIT must be adhered to. Where new or additional remote or homeworking methods are required, the access methods must be signed off by the IT security officer and a Service Directorate representative.

Section 7 - Computer and network management

7.1 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. *(see also 8.4.)*

As a minimum, system documentation should include, where appropriate, the following:

- Start up and close down procedures
- Inter dependencies with other parts of the IT infrastructure
- Support contacts
- Back up procedures
- System recovery procedures
- Network diagrams
- Design documentation

7.2 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:

IT Administrators; System Administration; Database Administration; Systems Users, Audit.

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). 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. Where segregation of duties cannot be enforced, managers are to monitor the arrangement closely and report any anomalies immediately.

7.3 External contractor management

The use of external contractors/companies to manage or support 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. *C*ontracts should, as a minimum, comply with the measures set out in this policy and comply with the code of connection for third-party access to the corporate network.

All equipment is to be maintained to ensure its continued availability and integrity. Maintenance agreements are to be in place to ensure that equipment down time is minimal and guidelines regarding the removal of equipment for off-site maintenance are strictly adhered to. No sensitive information should be held on equipment that is due to leave council premises.

7.4 Operational change control

The Council shall have formal change control management responsibilities and procedures in place to ensure satisfactory control of all changes to equipment, software and procedures. *(see also 8.4.)*

7.5 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, including different products at the gateway and desktops.
- Ensuring that all users and members of support teams who use 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 (see section 6.6)
- 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. Anti-virus scanners will be configured to update daily or as often as practicably possible.

Irrespective of medium, (for example: diskettes, 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 (notwithstanding the protective measures being taken) a virus does enter the Council network then this shall be dealt with effectively and promptly by IT so as to minimise risk to the organisation.

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

- They report any suspicious incidents immediately by (in the first instance) contacting the IT Helpdesk team
- They follow any instructions received from the IT Department regarding dealing with a virus threat.

7.6 Vulnerability and Patch Management

The IT Department is responsible for keeping abreast of identifications of new vulnerabilities that could impact Council Information Technology Assets and for implementing patches accordingly. The IT Department is responsible for ongoing daily monitoring of new vulnerabilities.

For Microsoft Windows products Microsoft Software Update Services will be used for automatic updates. A Microsoft Software Update server will be configured at Council, and this server will be configured to automatically acquire software updates from vendors on a daily basis, and applied in accordance with the Council's patching policy.

For all other products, periodic checks will be conducted on a regular basis (at least weekly) to ensure that new vulnerability threats are identified and dealt with in a timely manner. Vendor websites will be checked, as well as both the SANS web site (www.sans.org) and also the CERT website (www.cert.org) on a weekly basis.

In addition, the IT Department shall 'run' an approved Vulnerability Scanning software tool on a quarterly basis. The IT Manager shall review the results of each scan and shall take appropriate action in the event that scans reveal an unacceptable level of risk. A risk treatment plan will be monitored to ensure appropriate mitigations are completed. Furthermore where the responsible individual makes a determination that there is a potential impact associated with a new vulnerability they shall immediately contact the IT Manager and determine an action plan. The action plan will typically comprise:

- Risk assessment – taking any 'mitigating' factors into account
- Further research with a security advisor who is familiar with the Council network (if appropriate)
- 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.

7.7 Data back up

In line with Business Continuity Planning procedures, adequate backups must be taken to ensure that all essential data can be recovered in the event of a computer disaster or media failure. These procedures are as laid down in the Council's Business Continuity Manual/Disaster Recovery Procedures and monitored by the IT Security Officer.

Back up arrangements for individual systems must meet the requirements as laid down in the above mentioned Business Continuity/DR Procedures or system administration documentation. A copy of backup procedures can be obtained from the IT Security Officer.

Backups will be tested weekly to ensure that they are able to be restored into a live environment in the event of a DR invocation.

7.8 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 IT, in line with the Corporate IT Strategy. In particular network segments that form part of, or are attached, either directly or indirectly to the corporate network shall:

i. Be installed, adapted and maintained in accordance with current, approved British and International Standards and codes of practice.

ii. Be designed and tested using best practice

iii. Be of a standard approved by IT.

iv. Not be adapted or altered in any way without prior consultation and agreement with the IT team under change control procedures.

v. Be only installed/adapted by contractors drawn from IT's list of Approved Suppliers.

vi. Utilise hardware components that have been selected from IT's list of Approved Products.

Responsibility lies with IT for any network installations planned to connect with the corporate network and will, before connection is established:

a. Be subject to acceptance testing and health checks to ascertain compliance with the standards detailed above.

b. Risk evaluation of the impact and scope of the change at an early stage of the project.

c. Be approved by the IT Manager and/or his delegated senior personnel, who has total responsibility to refuse to corporately connect to the network any such installation/machine which does not comply with the required Corporate network and Information Security Policy standards.

Any installations found not to comply with the above will be removed from the said network and appropriate investigations/actions taken to ascertain how that installation was connected to the corporate network infrastructure.

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 and controls, and their implementation, should, where possible, align with the manner in which the organisation does business.

Configuration shall reflect the following core security principles:

- Defence in depth: Do not rely on one layer of security, for example ensuring a secure perimeter at a firewall level while neglecting to keep internal machines patched. Systems should be configured securely at all levels.
- 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. Ensure that data flows through secure channels.

The Council’s IT infrastructure will be segmented such that there are at a minimum two main divisions, the ‘internal network’ and the "de-militarised zone" (DMZ). The DMZ will lie in between the internal network, other trusted external networks and the Internet such that there is appropriate segregation and network controls between networks. Firewalls shall separate networks restricting access to the minimum required levels. All equipment owned and/or operated by the Council for which direct external Internet connectivity is allowed, (be this an incoming or outgoing connection) will lie in the DMZ. The architectural models applied will be in compliance with Central Government guidance.

Configuration requirements for the following components of the IT infrastructure are set out in the build documents including:

- Configuration of DMZ equipment
- Server configuration
- Desktop configuration
- Thin client configuration
- Configuration of mobile devices
- Configuration of routers and switches
- Configuration of firewalls
- Configuration of the Wide Area Network
- Configuration of Wireless networks (including staff ang guest access)

7.9 Security of system documentation

System documentation may contain a range of sensitive information (description of application processes, procedures, data structures etc.). These must be held securely and subject to control procedures.

7.10 Disposal of media

Sensitive computer media must be disposed of securely when no longer required. It is the Council's practice to have a "confidential waste" collection system whereby all confidential documents are shredded.

When a hardware asset is decommissioned, the IT Department shall ensure that all information stored on decommissioned hardware and storage media (disk drives, tapes, floppy disks, CDs, memory, hard copies) 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 and Government guidelines.

7.11 Electronic mail

Electronic mail (e-mail) is now one of the primary methods of communicating with the Council, and within the Council by its employees.

Different email channels are provided and users are required to ensure they understand the purpose of each type of email and the types data of data e.g. classification which are appropriate for each channel.

All employees and members of the Council should ensure that information communicated via e-mail is accurate and care must be taken to ensure that they cannot be misconstrued and that the correct recipients are identified. As well as Data Protection considerations e-mail communication is another form of publishing and libel laws also apply. Employees may be personally liable for this. It may be the employee's responsibility to show that they were not the author of statements emanating from Work Stations/PC.

7.12 Dissemination of Council Information

Dissemination of Council produced information, shall be authorised according to the Council's policies pertaining to release of information to the public or other external bodies. It is the responsibility of management to know and adhere to these policies and procedures. Both the IT Security Officer and senior management will monitor this to endeavour to prevent the release of unauthorised information.

7.13 Security of electronic office systems

Electronic office systems (e.g. Microsoft Outlook) provide employees with the opportunity to easily share and pass information. Users of such systems must safeguard against unauthorised access of their diaries, e-mail, word processing documents and spreadsheets by ensuring that any read/write access rights are set at the correct level. Further information concerning this is available from the IT Security Officer and/or the IT Helpdesk.

7.14 Internet/ Intranet Facilities

The Internet/Intranet facility is provided by the Council to help staff perform their work efficiently and effectively, so that they can carry out specific research during the course of their work, learn about the application of new ideas/technologies and evaluate these effectively for possible Council business usage.

Dissemination of Council produced information, using the Internet/Intranet service, shall be authorised according to the Authority's policies pertaining to release of information to the public. It is the responsibility of management to know and adhere to these policies and procedures. Both the IT Security Officer and senior management will monitor this to ensure no unauthorised information is released.

Users are entitled to use the internet for facility reasonable personal usage in their own time. Further guidance is available from IT.

7.15 Public Service Network (PSN)

The PSN is a Central Government provided network to provide OFFICIAL access to Public Sector information. To retain access the Council is required to demonstrate compliance with controls determined by the Government.

Some services on the PSN are provided by agencies with further stipulations regarding technical and user access controls. Further guidance is available from IT.

7.16 Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a standard for organisations that handle credit/debit card information. It is a mandatory requirement for the Council to adhere to the set of requirements which will help to ensure the security of all card data and reduce the risk of fraud.

The standard requires that network controls and requirements are in place, and they will be monitored in accordance with the standard.

7.17 Data Encryption

The Council is responsible by law for all its systems, files and data being used on all its servers, networks, Work Stations/PC's, Laptops, Telephone Services and other related electronic technologies being applied. As such the use of these has to be controlled, monitored and supported in-line with good practice, legislative constraints and relevant security protocols.

Where is it not possible ensure the security of Council data through physical, procedural or other controls, for example in transit over a network or on mobile device, and the data is not in the public domain, data should be encrypted to an appropriate standard. This includes, but is not limited to:

- Internet services
- Mobile devices e.g. laptops, tablets
- Removable media e.g. USB devices, DVDs
- Email encryption and/or over secure channels.

7.18 Monitoring and Logging

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

As well as alerting the IT Department to suspicious activity within the IT infrastructure, logs provide an audit function that allows the IT Department and system administrators to review compliance with security policies (e.g. access control).

All event logs generated are to be collected in the SIEM. and be kept for a minimum of 6 months. Logs are to be monitored for anomalous events using appropriate software tools and categorised in order to determine the severity of the event, and to aid filtering and auditing of log files.

7.19 External 'Cloud' solutions

Cloud or remote data centre services are provided via the internet or secure connections to remote data centres provided by suppliers. This includes different models such as:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

With the increasing availability of 'Cloud' solutions and software employees need to be made aware of the risks and issues with implementing 'cloud' to provide business solutions.

However, there are many issues that need to be considered including:

- Data Protection Act 1998 compliance
- Compliance with Government guidelines on 'Cloud' solutions
- Impact on data sharing arrangements with third parties and their requirements for storage
- Control of data
- Business Continuity
- Exit strategies
- Security levels for application and server and data

Any Cloud solutions will therefore need to be approved by the IT Manager and where appropriate the IT Security Group prior to being used operationally.

Section 8 - System Access Controls

8.1 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.

Controls for authenticated users shall be driven by the "principle of least privilege", i.e. only that required to perform their duties: The associated procedures also need to be sufficiently flexible to enable changes to be made to a user's access privileges rapidly and efficiently to meet the needs of a dynamic working environment. Controls aimed at preventing malicious third parties gaining access to the company's systems and data are achieved through strong authentication procedures.

Each Assistant Director must be satisfied that all information (electronic and paper based) used throughout his/her service area has been approved and audited for correct usage (i.e. roles based access rights relating to information have been determined). It is prudent for each service area to maintain a documented *"Statement of Requirement"* to aid this process that shows permitted access rights. User permissions must be documented in central IT systems and a copy held securely.

8.2 User and login id. Sign-on/Registration

Access to the Council's IT services is controlled through a formal user registration process with the system owner. Access to services will not be permitted until the employee has adhered to the 'sign-on/registration' process as laid down in this Information Security Policy and IT's current User Sign-on procedures and the person is appropriately security-cleared to access the information on the system.

Login ids should be standardised and this will be formulated by the IT Security Officer.

Each user account will be established in accordance with the following procedures

- A new user account granting access to the network shall only be implemented by the IT Department following approval by the user's manager (or another responsible senior manager).
- When establishing a user account, the IT Department shall only implement those access rights specifically required to enable the user to perform their job function and as approved by that user's manager
- New accounts will remain disabled until such time as the new user has confirmed agreement to abide by the Council's Information Security Policy
- Unless otherwise specified, new user accounts for employees created under this Procedure shall be of indefinite duration, however, they are to be tailored to the individuals specific needs and working hours. Accounts for Contractors, temporary staff/volunteers/people carrying out work experience

and visitors shall be set with a specific expiry date. Any extension of time requires a modification to the user's account as per section 7.3 below.

- The IT Department will at all times keep complete records of user access rights and profiles and review at regular intervals (not exceeding 6 months)

All user accounts will be suspended after 90 days of non-activity, if no specific prioritisation has been placed against this user account.

8.3 Modifying Existing User Accounts

A modification to an existing user account shall only be implemented by the IT Department following approval by the user's manager (or another responsible senior manager). When modifying an existing user account, the IT Department shall only implement those modifications specifically approved by the user's manager.

When modifying an existing user's access rights, the IT Department shall:

- Verify with the user's Manager that the modified access requirements appear consistent with changes to the user's tasks.
- Ensure that previous access rights no longer required are removed.

Where there is a modification caused by a change in an employee's role, the user's existing manager should be consulted to determine access that is no longer required, and the employee's new manager (if applicable) should be consulted to determine newly required levels of access.

The IT Department will ensure that its records are updated following all modifications of a user's access rights.

8.4 Termination of User Accounts

User access to the Council's network is to be discontinued immediately when an employee leaves or a contractor, temporary member of staff/volunteers/people carrying out work experience or visitor completes their assignment.

The following procedures shall apply:

- The IT Department shall disable a user's access rights when the user's manager (or the Human Resources Department) gives notification to the IT Department. This shall occur immediately when an employee leaves or a contractor, temporary member of staff or visitor completes their assignment.
- A confirmation email of the removal of the account will be sent by the IT Department to Human Resources and the user's manager.
- The IT Department will ensure that a user's access rights are disabled on the date indicated in the notification to terminate. This should be accomplished by resetting the password immediately. Where the user has a mail box, this will be set to the "Out of Office" automatic reply for 30 days following the user's departure. The exact content for the 'Out of Office' auto-reply is to be provided by the user's manager.

- Three months following the disablement of a user’s access rights, if the role of that user has not been refilled, the user account will be fully terminated by the IT Department. At this time, the following shall occur:
    - The log in rights associated with that account shall be fully removed
    - All files in that user account shall be archived.
    - The email boxes associated with that user account shall be removed.

The IT Manager will make spot checks of a sample of leavers on a six monthly basis to ensure that the procedures for termination of accounts are being followed.

8.5 Privileged User Accounts

In order to ensure efficient administration of the Council’s IT infrastructure, it is necessary for certain members of the IT Department to have additional access rights beyond those of a “normal” user. This is known as “Privileged Access”.

The IT Manager will establish and manage a series of roles for members of the IT Department. For each role there will be a series of defined privileged access rights, which will be explained to members of the IT Department.

The current set of roles and access rights are in Appendix C.

All members of the IT Department granted a privileged access user account will also have their standard user account. The privileged access user account will only be used when performing activities specifically requiring the privileged access: for all other activities privileged users will use their standard user account.

8.6 Remote Access

Remote access to the Council’s network is necessary to enable third parties to provide technical support and services to the Council, and also in certain circumstances for employees who need to access the network when away from the office.

However, remote access potentially provides hackers with an entry point into the trusted network, and therefore needs to be managed in a secure way.

The IT Manager shall ensure that all remote connections for users are established and managed in accordance with the Council’s procedures. Further guidance can be found in the Remote Working Guidance.

Remote access requirements for third party service providers are covered in Information Security Policy section 2.5.

8.7 Authentication/Password Management

User Authentication is the principal means of validating a user's authority to access a computer service and the primary means of auditing the access to systems. Passwords are a key aspect of the authentication process. The IT Security Officer/IT controls all corporate systems, administrator passwords and specific departmental systems. In all other cases delegated security personnel will be appointed to control these via the IT Security Officer/IT Security Group/Head of Service.

Further details on passwords are shown in the Authority's Password Guidance.

8.8 User Responsibilities for Passwords

Users of IT systems must follow the Council's Password Guidance in the selection and use of passwords.

It is the responsibility of all employees/users of the Council's IT systems to maintain password security. Ensure no passwords are issued to unauthorised personnel. Passwords should not be divulged for any purpose.

If passwords are recorded they must be stored with a level of security commensurate with the password itself, and it should not be easily possible to determine its purpose from the information recorded.

All laptops, portable devices and smartphones are to be protected with a boot-up and Hard Drive encryption password. Devices will be approved by IT in accordance with PSN guidance.

8.9 Network access control

Network users, may only access the services and information for which they have been given authority to use. Access to systems must be controlled though access control software.

For external access to the network this will be controlled using two-factor authentication and secure network connection. Solutions for accessing the network will be assured to a classification of data. Data with a higher classification than the remote access solution is not permitted.

8.10 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 and the golden rule that should be applied is that if you are in any doubt as to which documents you may access, you should seek advice from your manager, Assistant Director, the Council Data Protection Officer and/or the IT Security officer. Access control groups must be used to enforce permissions to access documents and file shares.

Employees and Members of the Council will have access to Council documents and/or its information contained there-in where there is a business reason to have access.

Where information is classified at the level of OFFICIAL-SENSITIVE, access will be granted on a ‘need to know’ basis, authorised by an appropriate manager.

In any event, the employee or Member access to such documents or other information will be prevented if the information: -

- Is protected from disclosure as a result of probable or current legal proceedings and the City Solicitor advises that disclosure to the employee or Member concerned is likely to damage the Council’s position;

- May assist in personal or professional interest of the employee or Member concerned, which is not relevant to his/her Council duties.

- The advice of the City Solicitor will be sought when there is any doubt about an access to a document or other information. If, after receiving advice to the contrary, an employee or Member still wishes to obtain access to a document and/or information, then the City Solicitor will decide on the issue, subject to legislative constraints.

- The IT Security Officer/IT will ensure that any Council Information assets; are kept securely and not released to anyone who is not entitled to see them.

The Member: Officer Protocol in the Constitution contains further information in relation to this.

8.11 Enforced path

The route from an employee/users terminal or Work Station/PC to a specific IT service is controlled. The network is designed to allow for maximum scope for sharing of resources and flexibility of routing, but also, if breached it can provide the opportunity for unauthorised access of such IT facilities. It is therefore essential to limit the routing options at each point in the network through pre-defined choices. The IT Security Officer/IT will be able to advise on this accordingly.

8.12 User Authentication

Connection to any of the Council's IT services from external facilities is strictly controlled via appropriate proprietary authentication system software, through which the employee/user is validated before access is granted.

8.13 User Identifiers

All employees/users must have a unique identifier (user-id), this is to ensure that activities can be audit logged and any output can be successfully routed. The person to whom they have been issued only must use them. (see 7.2)

8.14 Use of System Utilities

Most computer applications have several system utility programs that may be capable of overriding system and application controls. Both the system manager/administrator and the IT Security Officer strictly control the use of these.

8.15 Security Breaches

The IT Security Officer will take immediate action to withdraw access prior to investigation where a breach of security may have occurred.

Section 9 - System Development and Maintenance

9.1 Security Requirements, Analysis and Specification

The IT Security Officer 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.

9.2 Information Records Requirement

Data input to applications must be validated to ensure that it is correct and appropriate. When specifying, implementing or reconfiguring systems it is important to take into account the Council's information records management policies.

9.3 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 systems are changed in a controlled manner. 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.

9.4 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 or the business. Version control and a record of all patches applied will be maintained in-line with the current change control procedures.

9.5 Restrictions on changes to software packages

Where modification to software packages is essential an impact assessment 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. Refer to the IT Security Officer for further information. In addition full documentation should be supplied.

9.6 Development, Test and Operational Systems

Where possible, development and test facilities / systems shall not be connected to an Operational system without formal accreditation and/or authority from the IT Security Officer. In instances where test and development facilities cannot be segregated completely, controls shall be put in place to ensure there is no impact on live services. All out-sourced development shall be rigorously tested prior to implementation.

Section 10 - Business Continuity Planning (BCP)

Inevitably services may fail on occasions and the duty for the Council/IT is to resume business continuity immediately, whilst reviewing the reasons for this failure of service and making appropriate changes where necessary.

BCP involves identifying and reducing the risks and impacts from deliberate or accidental threats to all the Council's vital services, ensuring that the delivery of critical services in particular is established within specified timeframes to an acceptable predefined minimum delivery level.

Please refer to the Council's BC/DR plans for further information, subject to appropriate Security clearance i.e. Member of the BC team, Incident Management Team, IT Team and any other staff deemed necessary by these bodies on a 'need to know' basis.

The BCP manual/process covers:

(i) Identification and prioritising of critical business processes.

(ii) Determining the potential impact of various types of denial of resources.

(iii) Identifying and agreeing all priorities, roles and responsibilities and business continuity solutions and arrangements.

(iv) Documentation of agreed procedures and processes.

(v) Education of all members of the IT recovery team.

(vi) Testing the BCP/DR plan annually with the minimum of a desktop exercise.

(vii) Reviewing and where necessary updating the BCP/DR plan as a minimum on an annual basis.

(viii) Off-site storage of the Business Continuity Plans, DR materials, back-up tapes/disks etc. being kept at a remote secure business location designed to protect such materials.

(ix) Corporate change control procedures to the BCP/DR plan.

10.1 Disaster Recovery Plan (DRP)

The business continuity plan for the IT Team incorporates the IT Disaster Recovery Plan for the Council. Due to the dynamic environment of IT this plan it is in constant development to meet the identified prioritised needs for the Council's recovery plans. The plan is corporately monitored through integrated performance monitoring and through the business continuity risk register.

The plan incorporates the following:

(i) Immediate procedures covering initial assessment and recovery initiation.

(ii) Short-term recovery procedures.

(iii) Long-term recovery procedures. This section deals with the restoration of a near normal service from temporary accommodation and forms the main body of the plan.

(iv) Permanent reinstatement procedures.

(v) Preventative measures and current IT security procedures. This section includes the procedures dealing with current IT security and operational practices which are designed to reduce the risk of a disaster and limit its impact in terms of recovery.

(vi) **Appendices**. These include schedules of suppliers, equipment and software, names and addresses and other IT Physical/Software Network Configuration material's etc. along with appropriate reference material where necessary.

(vii) **Testing procedures** and recorded evidence of regular testing

Section 11 - Compliance and Audit

11.1 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 number of specified machines or users.

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 Information Security Policy to ensure compliance with all legal obligations and to further ensure that no copyright material is copied without the owner's consent.

- Copying of software written 'in-house' by Council employees/contractors for use on its Work Stations/PC's comes under the same policy restrictions. Any copying of such material to Work Stations/PC's, Laptops etc. not controlled by the Council will also be an infringement of copyright.

- Where it is necessary to use a software product on additional machines, licences must be extended or additional copies purchased.

- The IT Security Officer is responsible for all such copyright material and monitors, controls, and further maintains a register/database of all copyrighted licenses accordingly.

It is the responsibility of the IT Security Officer and designated IT personnel, along with employee responsibilities to ensure that this software license inventory is regularly checked. It is the responsibility of the IT Manager to ensure that software without appropriate licences are not installed on any devices..

11.2 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 retention period, in a secure manner in line with the Information Security Policy and adopted procedures there-in.

All Departments are required to develop and maintain a Retention and Disposal Schedule and a period of time for which they must be retained. This information should then be passed to the Data Protection Officer, the IT Security Officer and Internal Audit for appropriate compliance monitoring.

11.3 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 has a Data Protection Officer who manages specific queries and compliance with the Act. The Data Protection Policy is available on the Council's Intranet.

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 Data Protection Officer or the IT Security Officer will also advise on the IT Security considerations as laid down by the Act.

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

11.4 Prevention of misuse of IT facilities

All of the Council's IT facilities are provided for business purposes only.

Any use of the Council's IT facilities for non-business or unauthorised purposes may be regarded as "*improper use of the facilities"*. If usage monitoring or other means identifies such activity, it will be brought to the attention of the Head of Service for that area concerned and appropriate disciplinary action taken *in-line* with the Information Security Policy and current Council disciplinary procedures.

However, equipment owned by the Authority may be used for "private" use providing that authorisation has been obtained from the Head of Service and reviewed by the IT Security Officer, to ensure IT security compliance.

Specific policies for use of Email and Internet Acceptable Usage are available through the Council's intranet.

11.5 Compliance with the Information Security Policy

Owners of all Council information must hold regular reviews of the compliance of their systems with the IT Security Officer, the IT Security Group, IT, and Heads of Service, in order to meet the Council's Information Security Policy, Standards and other security legislative and non-legislative requirements.

11.6 System Audit Controls

IT 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.

11.7 Protection of System Audit tools

Any IT Security and Audit tools, Computer Assisted Audit Techniques software (CAATS) and/or data etc., must be safeguarded to prevent any possible misuse or compromise. All audit logs, including System Administrator and System Operator, are to be stored securely, backed-up and protected according to the classification of the information. Any faults or anomalies are to be thoroughly investigated and any appropriate action carried out. Access to these logs is to be strictly limited to the IT Security Officer and/or nominated deputy.

Section 12 - The Council’s Disciplinary Process

12.1 Disciplinary Process

In all cases breaches of the Information Security Policy will be dealt in-accordance with the Council’s disciplinary procedures process.

This process is a deterrent to employees who might be inclined to disregard the IT 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 IT security.

For further information please refer to your copy of the Council's disciplinary processes and procedures; copies can be obtained from your manager or Human Resources or on the Council’s Intranet.

APPENDIX A - List of relevant legislation

- **Data Protection Act 1998**
- **Copyright, Designs and Patents Act 1988**
- **Computer Misuse Act 1990**
- **Health & Safety Act (Display Screen Equipment) Regulations 1992**
- **Trade Marks Act 1994**
- **Human Rights Act 1998**
- **Public Interest Disclosure Act**
- **Regulation of Investigatory Powers Act 2000**
- **Obscene Publications Act 1959 & 1964**
- **Freedom of Information Act 2000**
- **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**
- **Local Government Act 1972**
- **Local Government (Records) Act 1962**
- **Public Records Act 1958 and 1967**
- **Local Government (Access to Information) Act 1985**

APPENDIX B - Ownership of Information Systems

Application Name	**System Manager/Owner**
@PP (Licencing, ASB, EH, Tenancy, PS Housing)	Business Development and IT Manager
Achieve Forms	Business Development and IT Manager
Agresso Business World	Financial Services Manager
Cadcorp (GIS)	Business Development and IT Manager
CCTV	Community Services Manager
Choice Based Lettings	Housing Solutions Manager
Committee Management System	Legal and Democratic Services Manager
Contaminated Land	Environmental and Corporate Safety Manager
Council Mortgages	Head of Shared Revenues and Benefits
Council Tax	Head of Shared Revenues and Benefits
Electoral	Legal and Democratic Services Manager
Email	Business Development and IT Manager
ESP Bus Pass System	Customer Services Manager
EstatePro	Investment Manager
Gower/Web Services – crematorium	City Services Manager
Housing Benefits	Head of Shared Revenues and Benefits
Housing Rents	Tenancy Services Manager
ICES Parking	City Services Team Leader
IMPS Performance Management	Principal Policy Officer
IQPostme (Correspondence)	Business Development and IT Manager
JONTEK	Housing Support Services Manager
LACHS	Financial Services Manager
LloydsLink	Financial Services Manager
Metric Parking Office	City Services Team Leader
Midland Payroll	HR Manager
Mobile Device Management	Business Development and IT Manager
NetConsent (Policy compliance)	Business Development and IT Manager
NNDR	Head of Shared Revenues and Benefits
Openscape (Telephony)	Business Development and IT Manager
P2.net	Property Services Manager
Paxton – Door entry	Leisure, Sport and City Services Manager
PCF Bacs	Financial Services Manager
Pentana (Audit)	Audit Services Manager
Q-Nomy (Contract Centre Queueing)	Customer Services Manager
Uniform (Planning and Building control)	Planning Manager
Repair Locator	Tenancy Services Manager
Kirona (Repairs Scheduling)	Maintenance Manager

Application Name	System Manager/Owner
Safety Organiser	Environmental and Corporate Safety Manager
Searchnet	Business Development and IT Manager
Servitor	Maintenance Manager
Snap Survey	Principal Policy Officer
Universal Housing	Tenancy Services Manager
Voice Recording	Business Development and IT Manager
Website CMS	Business Development and IT Manager
WFM	Customer Services Manager

APPENDIX C - IT Roles and Responsibilities

	ROLES				
	IT Manager	**Principal IT Officer**	**Principal Business Analyst**	**IT Officer/ Helpdesk Operator**	**Senior IT Officer**
Asset/Inventory Management	✓	✓			✓
Licensing Management	✓	✓			✓
Network	✓	✓			✓
Core infrastructure (servers, IT suite environment)	✓	✓			✓
Major application delivery	✓	✓			✓
Security	✓	✓	✓		✓
Desktop application delivery	✓	✓			✓
Database management	✓	✓	✓		
Internet	✓	✓			✓
Core communications	✓	✓	✓		
Back Ups		✓			✓
Application development	✓	✓	✓		✓
Data Integration development	✓		✓		
Infrastructure integration development	✓	✓	✓		
User Administration		✓	✓	✓	✓

System administration (management of application users, data within applications etc.) for some applications is managed by Directorates to ensure an appropriate division of duties.