GUILDFORD BOROUGH

Information Systems Security Policy

Corporate Owner:	ICT Manager
Contact Person:	Adrian Hudson
Applicability:	All Staff
Original Issue date	January 2018
Current Version Issue Date:	September 2018
Version:	1.07

Revision History

Revision Version	Date	Author	Description
1.0	16th January 2018	Michael Hynes	Draft Text
1.01	17th January 2018	Adrian Hudson	Draft Review
1.02	25th January 2018	Adrian Hudson	Draft Changes
1.03	29th January 2018	Michael Hynes	Amendments
1.04	01st May 2018	Michael Hynes	Amendments
1.05	18th May 2018	Ciaran Ward	Amendments
1.06	24th May 2018	Michael Hynes	Draft for Approval and Consultation
1.07	25th September 2018	Michael Hynes	Final

Table of Contents

1 About This Document

1.1 Purpose

The purpose of this document is to define the policies and standards adopted by the Guildford Borough Council in respect of its use of Information & Communications Systems.

1.1.1 Associated Documents

This document should be read in conjunction with the following documents

- **ICT Password Policy – Advises on detail of Password Policy and includes guidelines for end users**
- **ICT Users Policy** (which explains how many of these policies are applied from the user's perspective.)

2 Information Systems Security Policy

2.1 Introduction

2.1.1 Overview

The purpose of this section is to define the Council’s policy direction in respect of Information Systems Security and to confirm the importance attached to this matter by the Council’s Corporate Management Team.

This document does not set out specific security procedures as these are defined in the various Procedures Manuals maintained by each operational Department or service within the Council. The policy does provides guidelines which should be applied and incorporated into procedures wherever appropriate and practical.

In general the policies defined in this document apply to all Services within Guildford Borough Council. Where local legislation or standards of practice require modification this is duly noted.

2.1.2 Definition of Information Systems Security

The purpose of security is to ensure **business continuity** and to mitigate **risks to the business** by preventing and minimising the impact of security incidents.

Information security management has three basic components:

- Confidentiality: ensuring that information is accessible only to those authorised to have access
- Integrity: safeguarding the accuracy and completeness of information and processing methods
- Availability: ensuring that authorised users have access to information and associated assets when required.

Information takes many forms - it can be stored on computers, stored in the Cloud, transmitted across public/private networks, printed or written and spoken in conversations. From a security perspective, appropriate protection should be applied to information in all its forms. This document addresses those aspects of information security which specifically relate to information held on computer systems.

2.1.3 Management Support for Information Systems Security Policy

The Council’s Corporate Managment Team:

- recognise the important role that I.S. security plays in ensuring the confidentaility, integrity, availability and of the Council’s critical computer systems;
- ensure that all business and personal identifiable information (including that held in computer systems) is properly safeguarded and

- are particularly aware of the need for strict compliance with legal, regulatory and contractual requirements which relate to computer security.
- Service Leaders are accountable for ensuring implementation of this policy within their services.

The Corporate Management Team therefore fully endorse the policies set out in this document and will take appropriate action to ensure compliance.
All staff are expected to comply and proactively engage with the implementation and operation of this policy

2.1.4 ISO/IEC – International Organisation for Standardisation/ International Electrotechnical Commission and Standard of Good Practice for Information Security 2016 (SOGP)

This section has been prepared with reference to the ISO/IEC 27001:2013 publication: "Information Technology – Security Techniques – Information Security Management Systems – Requirements" and "The Standard of Good Practice for Information Security 2016" (SOGP)

2.2 Responsibility for I.S. Security

2.2.1 Introduction

This section defines the overall responsibilities for I.S. security within the Council's organisational structure.

It is important to note that the success or failure of this policy relies upon all persons within the organisation treating I.S. security seriously and fulfilling their role diligently.

2.2.2 Managing Director and ICT Manager

The Managing Director and ICT Manager are responsible for:

- reviewing and approving the I.S. security policy;
- agreeing and supporting Council-wide I.S. security initiatives;
- ensuring that I.S. security is properly integrated with all other security related policies;
- promoting the Council's I.S. security policy and awareness throughout the organisation;
- approving the acquisition and/or development of new computer systems to ensure they meet the Council's business needs, with reference to the Corporate Management Team as appropriate.

Information Assurance are responsible for:

- independently reviewing I.S. security procedures and practice throughout the organisation and ensuring that they reflect the approved policy and are feasible and effective;

- providing advice to both the Council’s senior management and ICT Management on all matters relating to computer and information security;
- assessing and approving the logical and physical security procedures built into new computer systems (in conjunction with ICT Management);
- authorising logical access rights to all business sensitive computer systems as part of the approved procedures agreed for such systems.
- performing due diligence on third party suppliers that process data on behalf of the Council

2.2.3 ICT Management

ICT Management are responsible for:

- devising and maintaining the I.S. security policy and obtaining approval for any changes to it via the Managing Director or ICT Manager;
- devising effective I.S. security procedures and practices and consulting if appropriate (which reflect the Council’s policy) in respect of all computer systems and mobile devices for which they are responsible;
- implementing and ensuring compliance with all I.S. security procedures and practices for which they are responsible as defined in their Operations Manual(s);
- ensuring the physical security of all the computer equipment and media which is located and/or used in their Department or which they have overall responsibility for;
- providing advice to the Council’s senior management on all matters relating to computer and information security; assessing and approving the logical security procedures and consulting where appropriate built into new computer systems (in conjunction with Internal Audit);
- authorising logical access rights and consulting where appropriate to all business sensitive computer systems as part of the approved procedures agreed for such systems;
- acting in the role of Security Officer for business sensitive computer systems as defined in their Operations Manual;
- working with the Data Protection Officer in respect of the General Data Protection Regulation.
- ensuring that any software malfunction is resolved in accordance with the procedures defined in the Department Operations Manual to minimise the risk of information security breaches and consulting where appropriate

2.2.4 Office Services Department Management

Office Services Department Management are responsible for:

- providing, operating and maintaining appropriate physical security mechanisms and environmental controls to protect business sensitive computer systems.

2.2.5 HR Management

HR Management are responsible for:

- ensuring that all potential staff recruits are appropriately screened.
- ensuring that all employees and temporary staff sign a confidentiality (non-disclosure) undertaking.
- ensuring that terms and conditions of employment for all staff define the employee's responsibility for information security.

2.2.6 Service Leaders

Service Leaders are responsible for:

- implementing and ensuring compliance with all I.S. security procedures and practices for which they are responsible as defined in their Operations Manual(s);
- ensuring all staff in their Department comply with the policies set out in this document and with any specific instructions relating to I.S. security as specified from time to time by the Corporate Management Team;
- ensuring that job descriptions define all relevant I.S. security responsibilities;
- ensuring that all employees are given appropriate I.S. security education and training.
- ensuring the physical security of all the computer equipment and media which is located and/or used in their service.
- ensuring the security of all confidential or sensitive information (including personal identifiable data) held in any form, which is located and/or used in their service.
- ensuring that procedure manuals define appropriate retention periods for all documents that must be retained to meet statutory, regulatory or organisational requirements.
- reporting any suspected security incident or security weakness to senior management, in accordance with the procedures defined in the ICT Users Policy
- reporting any apparent software malfunction to the ICT Manager via the ICT Service Desk, in accordance with the procedures defined in the ICT Users Policy.

2.2.7 All Staff

All staff are responsible for:

- complying with all I.S. security procedures and practices defined in their Services Operations or Procedures Manual;
- complying with the policies set out in this document and with any specific instructions relating to I.S. security as specified from time to time by senior management;
- ensuring the confidentiality of all business sensitive and personal identifiable data that they have access to;
- ensuring the physical security of all the computer equipment and media which is located and/or used in their Department;

- ensuring the security of portable computer equipment and media which they use off the premises in accordance with the procedures defined in the ICT Users Policy;
- reporting any suspected security incident or security weakness to their Line Manager, in accordance with the procedures defined in the ICT Users Policy;
- reporting any apparent software malfunction to their Line Manager, in accordance with the procedures defined in the ICT Users Policy.

3 Compliance

3.1 Introduction

This section defines the Council’s security policy and practices to ensure compliance with all relevant statutory and contractual requirements.

Legislative requirements differ from country to country, therefore advice on specific legal requirements should be sought from the Council’s legal advisors as appropriate.

3.2 Compliance with Legal and Contractual Requirements

3.2.1 Software Copying

Copyright material must not be copied without the owners consent.

Computer software is normally supplied and used under the terms of a licence which may specifically limit the use of that software to specific machines or a specific number of users. The licence normally also limits copying of the software.

Under no circumstances should software be copied either for use on the Council’s premises or elsewhere without first making reference to the ICT Department and obtaining their authority.

The ICT Department are responsible for ensuring that software is used and copied only within the terms of the relevant licence agreement. A register of software will be maintained by the ICT Department and software usage audited on a regular basis.

3.2.2 Statutory, Regulatory and Organisational Records

Statutory, regulatory and organisational records must be retained in accordance with all relevant legal requirements.

Records processed by each business unit to be classified and retained in accordance with procedures defined for those records. Relevant retention periods are to be incorporated into procedures manuals and updated from time to time as necessary.

Service Leaders are responsible for ensuring the safe and secure storage of such records.

3.2.3 Compliance with Data Protection and Secrecy Legislation

Systems which process personal data (on individuals) must comply with data protection legislation.

All staff must comply with the terms of data protection legislation.

It is the responsibility of the "Data Controller" of any system to inform the Data Protection Officer about any proposals to keep personal information on a computer. The Data Protection Officer is responsible for maintaining the registration under local Data Protection legislation.

(Note that the "Data Controller" of a system is usually the relevant Service Leader which is responsible for maintaining data in any system which processes personal data.)

3.2.4 Misuse of ICT Services

Council ICT services including but not limited to hardware, software, printers and peripheral devices such as mobile phones and USB memory sticks must only be used for authorised business purposes.

Council ICT services are provided for business purposes. Their use must be authorised by management. Any use of Council facilities for non-business or unauthorised purposes (without management approval) may be regarded as improper use of the facilities.

3.2.5 Use of Cryptography

Use of cryptography must comply with all relevant legislation.

Some countries control the use of cryptography. Therefore before any cryptographic system is deployed its use must be authorised by the ICT Manager who must take due account of relevant legislation.

3.2.6 Compliance with Security Policy

Computer systems must be regularly reviewed to ensure compliance with the Council's security policies and standards.

Independent reviews of I.S. security should be carried out on a regular basis in respect of all business sensitive computer systems. These reviews may be undertaken by the internal or external auditors or by other specialist organisations.

Internal Audit are responsible for ensuring that such reviews are carried out on a regular basis appropriate to each system.

4 Physical & Environmental Security

4.1 Introduction

Security is a very important consideration for any computer system, but particularly so for the Council's system. Guildford Borough Council maintains security procedures and arrangements which are designed to counter the risks of:

- sabotage, vandalism and theft;
- fire, flood and power failure;
- unauthorised access to or amendment of live data and program files;
- incorrect or unauthorised processing.

This section is specifically concerned with those aspects relating to physical access to computer systems and the protection of computer hardware and media. These controls are over and above those employed in relation to the Council in general.

4.2 Secure Areas for Computer Hardware

All ICT computer hardware supporting critical or business sensitive systems must be housed in secure areas.

The main computers running the Council's business critical systems must be housed in secure areas. Such systems include: ;

- Any "File Server" hardware supporting business critical systems;
- Any equipment related to external communication links (e.g. Firewalls, Network routers or switches and Third Party equipment)
- Any Cloud based service .

4.3 Physical Entry Controls

Secure areas must be protected by appropriate entry control systems with access granted only to essential staff.

The Office Services Department are responsible for maintaining and issuing keys or electronic access cards as agreed with the local ICT management.

It is recognised that third parties will need access to secure areas for a variety of reasons. ICT management are responsible for ensuring that where third parties have physical access to secure areas and they also have log-in access to critical systems or security controlling systems (e.g. administrator login to servers, firewall devices or other security systems), that they are directly supervised by a suitably qualified member of ICT staff.

4.4 Equipment Siting and Protection

Equipment should be sited and protected to reduce the risks of damage, and unauthorised access.

Wherever possible and appropriate, critical computer equipment should be protected against potential hazards. The following methods of protection are recommended:

- fire & smoke detectors in all computer rooms
- fire extinguishers (suitable for electrical fires) in all computer rooms
- automatic fire extinguisher system in computer rooms (optional)
- water detectors in computer rooms (optional)
- additional air conditioning equipment (optional)
- regular specialist cleaning and environmental monitoring (optional)
- smoking, drinking and eating to be prohibited in computer rooms
- Where computer equipment requires a specially controlled environment then the temperature, humidity and power supply should be monitored. This will normally done automatically by the control systems themselves - with alarms indicating abnormal conditions. Any exception condition must be reported by the Computer Operators to the ICT Manager and Office Services Department management.

4.5 Power Supplies

Critical equipment must be protected from power failures or other electrical anomalies.

A suitable un-interruptible power supply (UPS) must be installed for all equipment supporting critical business systems.

The Office Services Department (or local equivalent) are responsible for ensuring that UPS equipment is regularly tested in accordance with the manufacturers recommendations.

4.6 Equipment Maintenance

Computer equipment must be appropriately maintained.

ICT Management is responsible for ensuring that all computer equipment is maintained in accordance with the supplier's recommendations.

Repairs and servicing of equipment must only be carried out by authorised maintenance personnel.

4.7 Portable Computer Equipment

Individuals using portable computer equipment off the Council's premises are responsible for the security of both the hardware and any software and data files held on the equipment.

The following guidelines should be applied by users of portable computer equipment.

- When travelling, equipment and media should not be left unattended in public places.
- Portable computers should be carried as hand luggage when travelling.
- Portable equipment should not be left at home for longer than is necessary to complete a specific piece of work.
- Equipment should be marked with a Council Asset Number which can be tracked.

4.8 Secure Disposal of Equipment

Data must be erased from all equipment and media prior to disposal.

Computer equipment must be disposed of in accordance with the Council's procedures for disposing of Fixed Assets. Additionally any data held on such equipment or on associated media (disks, tapes, cartridges etc.) must be destroyed securely prior to disposal.

Note: It is not considered adequate simply to delete data file directory entries as the underlying data can still be reconstructed. All Council assets will be managed by ICT and securely wiped or destroyed. If you are unsure about any other device, including personal equipment which may hold Council data such as portable memory sticks, you should seek advice from the Council's Information Assurance Manager before disposing of the item.

4.9 Security and Emergency Procedures

All security and emergency procedures must be properly documented in Operations Manuals and all staff made aware of these procedures.

Service Leaders (particularly the ICT and Office Services Departments) are responsible for ensuring that their Operations Manuals properly document the procedures to be followed in respect of all security and emergency arrangements.

It is important that all staff are trained and aware of the procedures to be followed in the case of any emergency and that appropriate notices explaining such procedures are prominently displayed.

5 Computer System Management

5.1 Introduction

This section specifies the level of documentation and procedures which must be maintained in respect of the Council's business sensitive computer systems. It also sets out the basic requirements for managing and operating the Council's computer systems.

These procedures are intended to ensure the correct and secure operation of the Council's computer systems.

5.2 Operational Procedures and Responsibilities

5.2.1 Documented Operating Procedures and User Guides

Documented procedures must be maintained in respect of the operation and use of all business sensitive computer systems.

Clear and comprehensive **operating procedures** must be maintained for all operational computer systems. These should cover:

- Basic hardware operating instructions (or cross reference to other manuals)
- Job scheduling requirements
- Output handling instructions
- Operational controls and checks
- Housekeeping and backup processing procedures
- Exception handling procedures
- System restart and recovery procedures
- Hardware and software support contacts
- Operations and backup logging/recording requirements

ICT Management is responsible for producing and maintaining operating procedures and will normally be the responsibility of operations staff within the ICT Department to carry out these procedures.

As Guildford Borough Council generally use packaged off-the-shelf software, **user guides or manuals** will normally be provided by the software supplier. However where bespoke systems are developed it is the responsibility of the ICT Department to ensure that appropriate user documentation is produced.

5.2.2 Incident Management

Exception conditions (e.g. hardware failure, operational error, software fault) must be reported promptly to the appropriate member of management to minimise the potential impact of such incidents. A log of "operational risk" or "security incident" events must be maintained and reported to senior management (operational risk reporting) on a regular basis.

Hardware failures (except workstation PC's or terminals) must be reported to the ICT Manager as soon as they are discovered.

Operational Errors must be reported to the ICT Manager as soon as they are discovered.

Software faults (or suspected faults) must be recorded on an appropriate error reporting form and passed to the ICT Manager at the earliest opportunity. Where such faults are considered serious they must be advised urgently. The ICT Department must maintain a log of all such software error reports and ensure they are actioned in a timely manner.

It is the responsibility of the Service Leader to determine how any of the above problems are to be resolved and whether other Department Managers or senior management should be advised of the problem.

Serious incidents (i.e. those which may impact the Council's day to day operations) and any faults which cause incorrect data or information to be produced, should normally be advised to the ICT Manager and a member of the Corporate Management Team.

5.2.3 Segregation of Duties

The risk of negligent or deliberate system misuse will be minimised by appropriate segregation of duties.

Wherever possible the following functions should not be carried out by the same person:

- business systems user or data input operator
- computer operator
- systems development and maintenance (programming)
- systems administration, change management and security officer
- security auditor

Wherever business critical data (e.g. accounting data) is modified outside of business as usual processing in an application package, there should normally be "after the event" checks done by a person different from the one who made the changes. All updates of business critical data should be approved in advance in accordance with documented procedures.

In cases where systems are used to effect **funds transfers** the system must incorporate facilities to ensure that at least two persons are required to effect the release of funds transfer instructions.

5.2.4 Segregation of Development and Operational Facilities

Test and development environments should be segregated from operational facilities and appropriate change control mechanisms employed when changing "live" or operational systems (e.g. program changes).

Wherever possible system test and development environments should be segregated either physically or logically from operational environments. The following controls should be used wherever practical:

- separate hardware should be used

- secure and separate logical environments should be used if separate hardware is not practical
- the use of system utilities which may be used to modify data should be strictly controlled
- systems development staff should only have access to operational systems for purposes of providing technical support – use of such access should be logged and checked by an independent person.

5.2.5 External Companies

Guildford Borough Council may from time to time use external companies to process business sensitive data. In cases, where this is deemed necessary to meet a specific business requirement, the business unit sponsoring the use of such facilities is responsible for identifying with support from ICT the full security implications and ensure appropriate security controls are in operation.

Particular issues that must be considered include:

- access to sensitive data by non-Council employees
- the implications for business contingency plans
- the security standards to be specified and the process for ensuring these are fulfilled
- the responsibilities and procedures for handling exceptions and security incidents

5.3 System Capacity Planning

Advance planning is essential to ensure the availability of adequate capacity and resources to accommodate business growth and the requirements of new systems.

ICT Manager is responsible for monitoring all computer systems to ensure the provision of adequate capacity to accommodate business growth.

Service Leaders must ensure that ICT Manager and ICT Management are fully aware and involved in all business planning which involves the provision of new or additional computer systems.

5.4 System Acceptance

The implementation of new information systems, upgrades and new versions should be carefully managed to ensure they meet business requirements, are fully tested and accepted by end users and have appropriate documentation in place.

The Council's Project Management Standards should be followed whenever new systems are implemented or upgraded. These are designed to mitigate the risks involved in such implementation projects. Normally ICT Management will be involved in such projects and should ensure that appropriate standards are followed.

Additionally, Standards have been developed to minimise such risks and should be followed by anyone designing and implementing “user developed” systems using these tools.

5.5 Virus Protection

Virus detection and prevention measures and appropriate awareness procedures must be implemented to minimise the risk of damage and loss of data.

ICT Management is responsible for implementing appropriate measures to counter the risk of computer viruses. This will normally include running virus detection software on all systems which are “at risk”. Particular care should be taken in the case of PC based systems (especially “File Servers”).

All staff must follow the virus protection rules set out in the ICT Users Policy.

5.6 Network Security

Appropriate controls must be established in respect of all external data communications, Wide Area Network systems and Internet connections, to ensure the security of data and the protection of such systems from unauthorised use and access.

ICT Management must implement and maintain appropriate measures to ensure the integrity and security of the Council’s Wide Area Network links and for all external data communications connections including links to external payment systems and service providers. All proposals for network data communications systems must be notified to the ICT Manager who will co-ordinate and obtain approval for such systems and associated security measures as proposed by ICT Management***.***
Measures taken to protect network systems may include as appropriate:-

- access controls
- encryption
- fire-walls
- message authentication
- cloud based storage encryption
- anti-virus facilities

5.7 Housekeeping & Media Handling

ICT Management must implement and maintain appropriate “housekeeping” measures to ensure the integrity and availability of services.

5.7.1 Data and Software Back-up

Back-up copies of essential business data and software must be made on a regular basis and copies stored off-site.

ICT Management is responsible for ensuring that copies of all essential data and software are made on a regular basis and copies stored off-site, in secure conditions, to meet the requirements of Business Continuity Plans.

Where back-up copies are taken on a daily basis they should be stored off-site at the earliest opportunity, preferably on the same day.

For systems with separate “on-line day” and “end of day” processes it is recommended that backup copies of the data files are taken both prior to and after the “end of day process”.

Software must be backed up before and after each update. It is preferable if the appropriate version of the software is backed up with the corresponding data files as this ensures the integrity of the file structure if re-runs are necessary.

The number of backup generations (historical copies) that are maintained will depend upon the nature of the application however, a minimum of five generations are recommended for all systems. The Council’s main accounting systems will require more generations and in particular copies of data as at the month end must be maintained for at least one year.

Business users must not take backup copies of data home for storage. Where it is important to store backup copies of data held within Office Automation Systems or on Personal Computers off-site, then appropriate arrangements must be made with either the ICT Department or the Office Services Department. (See also ICT Users Policy.)

5.7.2 Operator Logs

Computer Operators must maintain logs of all work carried out.

Operator logs should include as appropriate:

- start and finish times for each main phase of operations
- details of any error conditions or exceptions and actions taken
- records of all data and software backups

5.7.3 Storage and Handling of Computer Media

Computer media, particularly that holding sensitive business data, must be carefully controlled and physically protected.

System Operating Procedures must define how computer media is to be used and where it is to be stored.

All backup media should be clearly labelled. This label should be used when logging details of backups.

In general the latest three generations of any backup media should be stored off-site in secure conditions together with a report (directory listing) showing the contents of each tape, diskette or cartridge. The next generation will be on-site being prepared for use and one other generation may be in transit.

Computer media in transit and off-site, must be stored in locked boxes clearly labelled and containing the Council's name and address.

5.7.4 Disposal of Computer Media

Media containing business sensitive or personal data must be disposed of securely when no longer required.

All media (disks, tapes, cartridges etc.) which may contain business sensitive or personal data must be disposed of securely (e.g. by incineration or shredding).

Controls must also be in place for the removal of Cloud based storage.

Note: It is not considered adequate simply to delete data file directory entries as the underlying data can still be reconstructed. All Council assets will be managed by ICT and securely wiped or destroyed. If you are unsure about any other device, including personal equipment which may hold Council data such as portable memory sticks, you should seek advice from the Council's Information Assurance Manager before disposing of the item.

5.8 Security and Use of Electronic Mail (E-mail) & Internet Services

The ICT Manager with advice from the Legal Department is responsible for developing and maintaining the Council's policy in respect of e-mail and Internet use.

Note: The Council's specific policy in respect of e-mail and Internet use is included elsewhere in this document.

5.8.1 E-mail Services

ICT Management must implement and maintain appropriate measures to ensure the integrity and availability of e-mail services.

Measures should ensure (as far as is practicable and cost justifiable):-

- the on-going availability of inter-office and external e-mail services (24x7)
- protection against inbound and outbound computer viruses
- publishing a disclaimer on all outbound messages (wording to be agreed with Legal Department)
- restrictions on inappropriate wording in e-mail messages
- secure and strictly limited and authorised access to e-mail services from outside the Council's premises

5.8.2 Internet Services

ICT Management must implement and maintain appropriate measures to mitigate the risks involved in providing Internet services.

Measures should ensure (as far as is practicable and cost justifiable):-

- protection against computer viruses
- logging and reporting internet use on a regular basis such that Department management can be made aware of potential inappropriate usage
- restrictions to limit access to inappropriate web-sites

6 System Access Controls

6.1 Introduction

Control of access to computer systems and the data held within them should be based on the requirements of the business, taking account of the sensitivity of the data as well as any contractual or legal requirements.

This section describes the Council's policy in respect of system access to ensure that:

- unauthorised access to systems and data is prevented
- the appropriate level of access is allocated to users
- access is granted only with proper authorisation
- there is appropriate segregation of duties and separation between staff with access to personal identifiable data (PII) data and others (to minimise possible conflicts of interest and to maintian "Chinese Walls")
- controls are not so rigid as to negate the business benefits of the system

6.2 User Access Management

6.2.1 User Registration and Password Management

Access to all multi-user ICT services may only be granted via the new employee procedures laid down in the HR New Starter process.

Formal procedures must be established to control the issuance of User Accounts and Passwords which provide access to all business sensitive multi-user systems. These procedures should at a minimum:

- require requests for User Accounts to be authorised by a Line Manager on a need-to-use basis;
- maintain a formal record of all users;
- ensure that staff leaving the Council's employment have their user records promptly disabled;
- require users to sign requests to indicate that they understand the conditions of use;
- require users to sign an undertaking to keep passwords confidential;
- ensure that where temporary passwords are issued (e.g. user forgets password) they must be changed immediately they are used;
- ensure that passwords are conveyed in a secure manner (preferably via personal communication between the user and the ICT Service Desk);

6.2.2 Contract, Temporary and Third-party Employees

Contract and third-party employees should not normally be granted access to modify live data or programs. Exceptions may apply for staff of companies providing hosted ICT services.

User Accounts issued to third-parties or contract staff should not normally allow them to modify live data or source programs. Where such access is required (e.g. for emergency system maintenance) then a qualified member of ICT should oversee the work being done or a formal process for authorising and confirming the work should be put in place.

Where contract or temporary staff are employed for any period of time to work on the Council's premises, then a user specific ID and password should be issued in accordance with the normal procedures for full time employees.

Where applications are managed on behalf of the Council by third-party companies, their staff may have access to production data and programs. In such cases there must be a formal contract in place which must include appropriate confidentiality clauses.

6.2.3 External Users

External users (e.g. customers) access to be Council's computer systems must be strictly controlled and subject to appropriate formal contractual terms.

Where external users (e.g. customers, software or hardware suppliers) are to be given access to the Council's computer systems special care must be taken to control the use of such access. Each application will have its own special requirements but the following issues should be considered.

- Formal contracts may be required to limit the Council's liability and to define the users obligations.
- User Accounts and passwords may need to be issued in two separate communications.
- The security of the underlying communications technology must be adequate for the specific application (consider the need for encryption).
- Additional controls, over and above those normally applied may be necessary (e.g. challenge/response logons, access time restrictions, remote node authentication).

6.2.4 Review of User Access Rights

User access rights should be reviewed at regular intervals.

Internal Audit, together with the appropriate system Security Officer, are responsible for reviewing user access rights on a regular basis (recommendation is annually as a minimum.)

6.3 User Responsibilities

6.3.1 Password Use

All system users must follow good security practices in the selection and use of passwords.

The ICT Password Policy contains detailed requirements however as a minimum users must be made aware of the following requirements:

- Passwords must be kept confidential (where shared user Accounts are used the password must be kept confidential within the work group).
- Users should not keep paper records of passwords.
- Passwords should be changed if there is any indication of password compromise.

6.3.2 Unattended User Equipment

Users should ensure that they do not leave terminals or PC's unattended whilst logged on to any business sensitive system.

Users must log off from any business sensitive system whenever they have finished using the sytem or if they are leaving the device unattended for an extended period of time. Where the desk is being left unattended for a short period of time it is not necessary to log off from the network or systems but the screen must be locked at all times.

6.4 Network Access Controls

6.4.1 Logon Procedures

Access to ICT services should be via a secure logon process.

The procedure for logging on to computer systems should be designed to minimise the risk of unauthorised access. Therefore they should normally include the following features:

- Passwords should not be displayed on screen
- System should auto-disconnect after predetermined number of invalid logon attempts (normally three attempts are allowed)
- Recording of all user logons and logoffs (including unsuccessful attempts)
- Strong password rules (to minimise risk of passwords being guessed)
- Previous users logins should not be displayed

6.4.2 User Identifiers

User Identifiers and Passwords should be issued to individuals.

Users should be issued with a unique system ID so that activity can be traced back to the individual.

In exceptional circumstances (where there is a clear business benefit) a shared user ID can be used. Management approval and documented exception must be granted in these cases.

6.4.3 Password Maintenance

Password systems must provide effective mechanisms to ensure that quality passwords are used.

The precise method of managing passwords will differ from system to system but the standards to be followed as closely as possible are set out in the ICT Password Policy document

6.4.4 Terminal Time-out

Inactive terminals should be timed-out to prevent access by unauthorised users.

An automatic time-out facility should be used for high risk or business sensitive systems which disables the use of a terminal if it is left unused for a certain period of time. The maximum timeout period for these systems will typically be no longer than 15 minutes in line with current best practice.

6.4.5 External Communication Links

Connections via public or non-company networks (e.g. Internet, Leased lines, PSTN, X.25, ISDN) must be strictly controlled and secured.

Any hardware or software feature which allows external devices to connect to the Council's systems must be strictly controlled. Each will have its own special requirements but the following issues should be considered.

- The security of the underlying communications technology must be adequate for the specific application (consider the need for encryption).
- Additional controls, over and above those normally applied may be necessary (e.g. challenge/response logons, access time restrictions, remote node authentication).
- Physical and logical on/off switches may be used to control access to communications systems (such features should be disabled when not in use).

Remote access via the internet to the Council's network by Council staff (or approved third parties) will normally be controlled by use of an SSL VPN connection together with use of a one-time password (normally using a suitable remote access token such as SafeNet).

6.5 Application Access Controls

Logical access to computer systems should be restricted to authorised users. This will normally be achieved by limiting users only to the areas of functionality (menu options) they require to do their jobs and by controlling the data rights (read, write, update) they are authorised to. The principal of “Least Privelege” should be applied

6.5.1 Information Access

Access to sensitive information should only be granted in accordance with business needs.

The Information Assurance Manager, together with the Service Leader and Internal Audit must agree appropriate levels of access authority to enable each individual user or group of users to perform their jobs.

These agreed access rights must be recorded together with the user registration records. (A simple form indicating which “user group” an individual belong to for system access purposes will provide this information if it can be cross-referenced to a more detailed explanation of the rights of the “user groups”.)

Users will normally only be granted access to the data produced by their own Team, Department or Service. Users will not normally be able to see the “folders” used by other Services.

If cross Department or Service access is required this will either be via transparently “open” folders (i.e. clearly accessible to all) or via specifically created “shared folders” with restricted security controls in place.

6.5.2 Use of System Utilities and Programming Tools

Access to system utilities and programming tools must be restricted to authorised users.

Access to system utilities such as the SafeNet console and programming tools must be restricted to authorised and properly trained personnel - normally within the ICT Department. The use of certain tools may need to be restricted further and their use recorded.

6.6 Monitoring System Access

Systems must be monitored to ensure compliance with access policy and standards.

Audit trails and logs of system access and other security events must be maintained by Information Assurance Manager and checked on a regular basis. Internal Audit will undertake spot checks to ensure that these procedures are adequate and are being carried out thoroughly.

7 System Development, Maintenance & Change Control

7.1 Introduction

It is essential that due consideration is given to the security facilities that are required in systems being developed for, or by, the Council. Security requirements should also be incorporated into Statements of Requirement for systems being considered for acquisition.

Once systems are in place it is important that appropriate procedures are in place to minimise the risk of developers deliberately or accidentally modifying live data or software.

7.2 Security Requirements of Application Systems

Appropriate security and privacy controls must be built into application systems.

When new systems are being designed or acquired due consideration must be given to the security facilities required to ensure they meet the standards set out in this policy as well as any business specific needs.

In particular the following requirements should be considered:

- Facilities to ensure appropriate segregation of duties and to control functional access.
- Audit trails and logs to record important events.
- Facilities to ensure and verify the integrity of the data held in the system (e.g. Balance reports, file update controls etc.).
- Compliance with legal and regulatory requirements.

7.3 Outsourced Software Development and Package Systems

When code or applications are sourced from third parties, due consideration must be given to ensure there is minimal risk of program error; the availablity of on-going support and the Council is not exposed to contractual or licensing risks.

Where software or program code is acquired from third parties, ICT management must ensure that:-

- appropriate licensing arrangements and intellectual property rights are defined in the licence agreement;
- escrow arrangements are in place to ensure access to source code in the event of the failure of the provider where required
- appropriate maintenance agreements are in place to ensure the ongoing support of the software
- software is thoroughly tested before implementation and final payment is made.

7.4 Separation of Development and Operational Systems

Development and testing facilities must be separated from operational systems.

Physical and/or logical controls must be established to ensure that development and testing facilities are separated from operational systems. Development staff must not be able to update live data or programs other than through strictly controlled and authorised procedures.

7.5 Change Control Procedures

Appropriate Change Control Procedures must be in place for all business sensitive systems to ensure the integrity of the data and programs used by them.

ICT Management in consultation with the Business must devise and maintain and implement Change Control Procedures for all business sensitive systems. These should ensure that:-

- Change requests are reviewed and authorised by the respective Service Leader, Internal Audit and senior ICT Management.
- System changes are thoroughly tested by both development staff and end-users.
- End-users "sign off" on changes as accepted before being implemented.
- A record of all changes are maintained.
- Appropriate program version control is maintained.
- Only the Service Leader or Internal Audit or Senior ICT Management can initiate the change control process.

7.5.1 Exceptional Data File Maintenance

It is recognised that the use of GIS and other mechanisms which directly update "live" data may be essential in certain exceptional circumstances. However it is also recognised that the use of these methods carries a high degree of risk and therefore the use of these methods must be strictly controlled.

Programming staff may be allowed use of the GIS utility and other similar tools - however they must NOT have "write authority" to "live" data files.

Where such tools are used to amend "live" data then a hard copy report of data changed (preferably showing before and after images) must be produced and signed-off by the Service Leader, or ICT Manager, or Director, and Internal Audit. These reports should be retained in line with the Council's record retention policy.

8 Business Continuity Planning

8.1 Introduction

The Council's Business Continuity Plans are designed to ensure that the Council's critical business activities can be restored as quickly as possible following any major disaster. These plans cover all aspects of the Council's business.

ICT is considered to be a critical service and therefore ICT Continuity Planning is a major element in the overall plan. Not only must the ICT Plan provide for major disasters affecting the whole business, but also for localised problems (e.g. hardware failures or power failures) affecting only the ICT systems.

8.2 Producing Business Continuity Plans

The Council's Business Continuity Plan must include procedures for recovering all of the Council's critical ICT services.

The ICT Continuity Plans for each Service should as a minimum provide:

- Off-site ICT facilities including appropriate computer hardware and communications equipment.
- Off-site storage of back-up data for all systems.
- Clear allocation of responsibilities for all staff involved in the recovery process (with due consideration for backup staff).
- Detailed emergency procedures which describe the action to be taken immediately following a disaster.
- Detailed recovery procedures explaining how to re-build the various ICT systems.
- Contact lists for staff and suppliers.
- Resumption procedures which explain the action to be taken to return to normal business operations.
- ICT Management are responsible for developing and maintaining these plans in accordance with the Council's requirements for the overall Business Continuity Plan.

8.3 Testing Business Continuity Plans

Business Continuity Plans must be tested and updated regularly.

The complete Business Continuity Plan for each operating unit will be tested on regular basis as appropriate to local business requirements. However it is recommended that the ICT section of the plan should be tested at least annually.

The test must be carefully planned to determine objectives and test results recorded and reported back to senior management.

The plan should be updated following each test to incorporate new systems, changed procedures, staff or organisational changes and any other relevant factors.

Local ICT Management are responsible for ensuring that ICT Continuity Plans are adequately tested and updated in accordance with Council procedures.