APPENDIX J

Security Policy
Contents

APPENDIX J

APPENDIX J

1. Introduction

The Management of Information is an integral part of the Council's activities and is becoming a major strategic asset to any organisation. Investment in equipment such as personal computers (PCs) and the communications infrastructure is significant. Because this is essential to the provision of services, policies and procedures need to be laid down and enforced in order to safeguard those services and the Council's interests.

These include:

- The physical assets
- Access to the information on those assets
- Services continuity
- Users of the systems and equipment
- Compliance with legislation

2. Objectives of the Policy

The objectives of the policy are

- to minimise any adverse risk to the Authority's Information Systems

- to protect the authority's IT systems infrastructure, hardware, software and information

- to ensure that they are kept secure and only available for proper and authorised utilisation.

3. Scope of the Policy

This Policy therefore applies to:
Individuals

- 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 & Communication Technology (ICT)
- All temporary and agency staff directly or indirectly employed by the Council
- All users having access 'of any kind' to The Authority's systems, resources and/or networks

Equipment

- PCs, Laptops and associated equipment, including tablets and mobile equipment
- Servers
- Telephone & data networks
- Software
- Relevant filing systems and all hard copy information
- All telecommunications equipment including mobile phones and smart phones.

This Policy applies to all information held by the Council irrespective of medium e.g. includes both electronic and hard copy and by extension, business related conversations and knowledge of staff members.

4. Enforcement

4.1. All users of the Council's ICT equipment and hard copy systems are responsible for compliance with this Policy.

4.2. In protecting the information assets, the Council will obey all applicable laws and regulations and charges its employees to maintain the highest ethical standards. **The Council views security seriously and any breach of this Policy could lead to disciplinary action being taken against those who commit this breach**.

4.3. Violations may be considered gross misconduct and as such may lead to the dismissal of the employee or employees concerned. Violations can include:

- The installation and use of unauthorised software or data (this includes any storage device i.e. floppy disk, memory sticks, cds etc.)
- The installation and use of any unauthorised computer or telecommunications equipment
- Unauthorised and/or illicit use of the Internet
- The use of data for illicit purposes (including violation of any law, regulation or any reporting requirement of any law enforcement or government agency)
- The copying of software which breaches copyright agreements
- The copying of any materials protected under copyright or patent law or make material available to others for copying
- Exposing the Council to actual or potential loss (monetary or otherwise) through the compromise of ICT security
- The unauthorised disclosure of confidential or personal information or the unauthorised use of corporate data
- Unauthorised personal use of equipment or changes to equipment configuration
- Unauthorised deletion or alteration of files or data which are business critical or to which the user has no right of access
- Avoidable damage to the Council's equipment
- Insecure usage and storage of information
- Frivolous use of computer resources which could overload and/or disrupt the Authority's network and/or storage limits
- Malicious or vexatious (untrue) statements made which damages the reputation of a person (or employer).

4.4. Any individual who has knowledge of a violation of this Policy must report that violation immediately to his or her line manager. Failure to do so could result in disciplinary action being taken.

4.5. In support of this policy all communication equipment will be subject to monitoring and auditing, in line with the Employment Data Protection Code of Practice.

5. Legislative Framework

5.1. The Council and all users/processors of information must comply with all relevant legislation and Council policies and procedures. Users may be held personally responsible for any breach of applicable legislation. Relevant legislation includes, but is not restricted to:

- 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

Anyone who is unsure of his/her responsibility should seek clarification from his/her line manager immediately.

6. Use of Council Communications Equipment and Networks

6.1. The use of the Council's Communication equipment for purposes not directly concerned with authorised Council business should only occur in line with the Personal User of Computers Addendum and Mobile Phone Policy.

6.2. ICT Services have the facility to monitor the access to the network. This facility may be used should a manager have reason to believe that the systems are being abused.

6.3. Staff may make the occasional personal telephone calls in an urgent situation or due to a personal requirement, which means that the communication is required at a specific time.

6.4. Staff will not use the Council's letter franking facilities.

6.5. Any abuse of the personal use of communication facilities may be subject to disciplinary action.

6.6. Access by outside bodies into any of the Council's networks or equipment is not permitted without prior recorded agreement between the IT Manager and the appropriate Head of Service / Strategic Director. Suppliers should complete the Third Party Access Policy before attempting to gain access.

6.7. Telephone numbers allowing access to the Council's networks must not be disclosed to unauthorised persons/bodies e.g. software supplier connections..

6.8. No equipment may be connected to the network or attached to any equipment connected to the network without authorisation from the IT Team.

6.9. Approved Trade Union activities will be deemed to be Council business.

7. Data and Program Ownership

7.1. Data Quality Policy

The aim of the Data Quality Policy is to ensure that with the help of standardised practices within the area of data collection, that the authority's data is accurate, complete and timely and that there is internal and external confidence in the data.

The aim is to ensure that data is recorded promptly and correctly at source and is fit for purpose. This will be supplemented by robust arrangements to ensure that the integrity of data is maintained through any processing. Finally, appropriate data quality checks will be performed – proportionate and cost effective – before information and conclusions drawn from this data are released. Policy States the definition of 'high quality data' if it is:

- Accurate (in terms of consistency & correctness)
- Up to date
- Quick & Easy to find
- Available when needed
- Stored securely and confidentially
- Free from duplication
- Free from fragmentation (held in a variety of places**)**

7.2. The Council's Data

(a) All computer programs and data resident on the Authority's hardware are for the sole use of the council in undertaking its business. Access by Members and employees is solely for this purpose.
(b) Therefore no expectation of privacy by employees for anything they create, store, send and receive using Authority's computer equipment, should be accepted. As such, the User expressly waives the right of privacy rights.
(c) Copying, alteration or interference with computer programs is not permitted, without the recorded agreement of the IT Section.

7.3. Data Protection Legislation

(a) Systems (manual or computer based), which process personal data about living persons, must comply with current data protection legislation. The person responsible for such a system must ensure that the Management of Information Officer has details of the system and how it will be operated.

(b) There must be no unauthorised disclosure of personal data. Personal data may only be disclosed when authorised by the officers who are responsible for the data in accordance with data protection legislation and Council policies and procedures. Disclosures (and all forms of data processing) must only be made in accordance with current data protection legislation.

(c) The eight data protection principles are:

1 Personal data must be processed fairly and lawfully.
2 Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with that purpose or those purposes.
3 Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4 Personal data must be accurate and, where necessary, kept up to date.
5 Personal data processed for any purpose or purposes must not be kept for longer than is necessary.
6 Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act.
7 Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against loss or destruction of, or damage to, personal data.
8 Personal data must not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures

an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

8. Access to Information and Communications Technology (ICT) Systems

8.1. General

The approval, implementation and control of all networks and systems are the responsibility of the IT Manager, in conjunction with user service areas. The creation and allocation of user rights within a system is the responsibility of the system administrator. The data contained within each system should be subjected to a risk analysis to determine its sensitivity and the impact of it being accessed by, or disclosed to, unauthorised persons. In the event that a significant risk is identified additional security measures will be implemented.

Systems containing personal or sensitive data that are being accessed from public or unsecured areas should be positioned in such a way that information stored or processed cannot be viewed by unauthorised persons and should be configured with time outs to ensure sessions are disconnected after a predetermined period of inactivity. Where this cannot be achieved cleanly due to the application design then password controlled screen savers will be configured on each PC at risk. Day-to-day management of each system may reside outside the IT Section as each system has a Systems Administrator (senior user), part of whose duties is to ensure adherence to the principles of access control.

The appropriate Systems Administrator (senior user) must be consulted before access can be given to that system. Requests for access to systems will be accepted only from authorised service area representatives.

Users will not be given direct access to systems over the Internet. All such access will be via the DMZ, Demilitarised Zone, an area of the network that stands between the outside world and our internal system. Data to be accessed by the public or external untrusted users will be located in the DMZ.

8.2. Password Controlled Access

(a) Each user must have a unique user-ID and password. The use of another person’s user-ID is not permitted. Users will not disclose their user-ID or password or visibly record them on or near equipment providing access to networks or systems.

(b) Where a default password is assigned to a user for first access, the user must change this initial password straight away.

(c) Passwords must be a minimum of eight alphanumeric characters in length. Passwords will be set to expire after 56 days and where possible password uniqueness will be deployed to prevent password toggling between two frequently used passwords.

(d) Unattended PC / Thin Clients must be either locked or logged out.

8.3. System Management

(a) Access rights for staff undertaking new roles and responsibilities should be assessed to ensure they are still relevant. The systems administrator(s) and IT Section where necessary must be notified immediately of any changes to systems access requirements.

(b) The IT Section and relevant systems administrators must be notified of staff intending to leave the employ of the Council. Staff must immediately have their access capabilities restricted as appropriate, and removed as soon as possible on leaving the Council.

9. Purchase and Disposal of Information Technology (IT) Equipment and Software

9.1. With the exception of minor or routine acquisitions and or replacements all requests for hardware and software must be approved by the ICT. The process will comply with the Authority's Financial Procedure Rules and the requirements of the EEC's public sector procurement policies.

9.2. The IT Service will only act on purchase requests from an Authorised officer (system administrator), evidenced through the submission of a Work Request.

9.3. Orders will only be made for equipment and software which comply with the Council's IT Strategy and which are appropriate for the users' business needs. Representatives from IT will consult with the user service area to ensure both these criteria are met.

9.4. Details of all IT equipment must be held within the IT asset database and maintained in accordance with the asset database management procedures defined in **Appendix 2**.

9.5. The disposal of all IT equipment, software and data storage media is the responsibility of the IT Section as defined in the Asset Management Procedures Document, **Appendix 2**.

9.6. Connection, disconnection or relocation of any IT equipment must be undertaken by the IT Section, as defined in the Asset Management Procedures Document, **Appendix 2**.

9.7. The IT Service will only act on disposal requests from an Authorised officer (system administrator), evidenced through the submission of a Work Request, as defined in the Asset Management Procedures Document, **Appendix 2**.

10. PC and Portable Computers

10.1. PCs and Portable Configuration (Including PDAs and mobile equipment)

Systems will be configured to allow users access only to those applications, features and facilities they require to perform their day-to-day duties. The IT Section will carry out the deployment and configuration of such equipment and where possible configuration will be standard across workgroups and locked to prevent unauthorised changes

10.2. Approved Software

Unlicensed or personal software must not be installed on the Council's hardware, or connected in any way to the Council's equipment or systems. Software deemed to be of use to the Council should be acquired by the Council under licence. Periodic checks will be conducted by IT staff and Internal Audit to ensure compliance with these provisions. (**See also section 7: Data and Programme Ownership; and section 14: Software Licences**.)

10.3. Data Storage Devices

Data storage devices (floppy disks, CDs, DVDs, memory sticks etc.) which have been used on other PCs, networked or otherwise outside the Council must not be used on PCs connected to the Council's networks, until the devices have been virus checked by the IT Section.

10.4. Unauthorised Equipment

Users must not connect personal or unauthorised equipment of any kind to the Authority's computer systems or networks without approval from the IT Section

10.5. Disposal of Equipment

All hardware including disks to be disposed of must be passed to the Council's IT Section.

11. Records Management

11.1. All hard copy information will be filed manually employing a relevant filing system. Retention and archiving of information shall follow the Council's adopted Retention Policy, which gives guidance on effective records management.

12. ICT Data Backups

12.1. It is the responsibility of Systems Administrators (senior users), in consultation with the ICT Manager, to ensure that appropriate back-up procedures are operated.

12.2. **Fault Tolerant Equipment** - For systems hosting critical information where ‘non stop’ availability is important, ICT have where possible deployed fault tolerant equipment such as redundant power supplies and highly available disk configurations.

12.3. **Backup Frequency** - The IT Section has made provision for all data to be held within various network storage devices that is secured on a regular cyclic basis. Any data not stored on the Network will not be backed up and will remain the responsibility of the individual user. The default backup frequency is every working day.

12.4. **Backup Media Storage** - The backup media must either be placed in a fire proof safe or removed from the physical environment of the system. Copies of backup media must be moved to another site on a daily basis. At least two full sets of media must be available at the off site location. Backup media must be clearly labelled

12.5. **Verifying Backup Media** - A procedure must be implemented to routinely read samples of the backup media on an alternative system to ensure the contents of the media are readable and contain the intended information

12.6. **User Profiles and Desktops** are not systematically backed up and users should not store documents in these areas as this will cause the logon process to take longer.

12.7. Individual files can be **restored**. Users should contact Steria for assistance.

12.8. **Email boxes** are backed up. However, due to the dynamic nature of the application, it is not always possible to restore individual emails. Users should make use of the deleted items facility to restore emails in the first instance.

13. New Systems, Modules or Development

13.1. ICT systems must not be acquired or developed without consulting the ICT Manager. This is to ensure that appropriate software and equipment is used to the standard appropriate for the business needs, and to ensure compliance with the Council’s IT Strategy and Procedures.

13.2. Suppliers will be expected to complete a pro forma detailing the impact of the change on the Council’s Infrastructure.

14. Software Licenses

14.1. Software misuse and theft is an extremely serious issue. The Authority will not condone the use of any software that does not have a license suitable to allow its use by Council staff, and any employee found to be using unlicensed software, or having unlicensed software installed on their IT equipment may be subject to disciplinary procedures.

14.2. All software must be installed by ICT Services to ensure compliance with software licensing rules and to ensure that there are no clashes with existing software.

14.3. It is the joint responsibility of the ICT Manager and System Administrators (senior users) to ensure that appropriate software licences are obtained and maintained.

14.4. The ICT Manager will ensure that, if the Policy laid out in this document is followed, the legal requirements of licences will be met. However, it is the responsibility of all service area managers to ensure that this Policy is followed at all times.

14.5.

15. Electronic Communication (including the use of the Internet)

15.1. Electronic Communication includes:

- Use of E-mail within the Council
- Use of E-mail to and from addresses outside the Council
- Use of the Council's Intranet
- General use of the Internet

15.2. **Access Authorisation** Prior to being connected, all users of Electronic Communication must have authorisation from their line manager

15.3. Officers must comply with the Council's Code of Practice relating to the use of Internet and electronic mail facilities (Acceptable Usage Policy **see Appendix 1**)**.** Specifically, the following points should be noted:

- Services will not be used to access, create, transmit or publish any material likely to cause offence.
- Authorised staff will monitor the content of e-mails and data that are transmitted to or from the Council's equipment or downloaded to the Council's equipment to protect the Council from legal infringements.
- All Internet sites visited are recorded automatically and may be interrogated should misuse be suspected.
- Data Protection legislation applies.
- Failure to comply with Council policies and procedures or relevant legislation may lead to disciplinary and/or legal action.

15.4. Internet and Intranet Access

Failure to follow this Policy may put the Council's data and networks at risk: therefore non-compliance may lead to disciplinary action. Access to the Internet and / or Intranet is only permitted on receipt of a properly authorised request form. Control of access within a department is a service area management issue. All access must be in a manner approved by and arranged through the IT Section.

15.5. ICT Services have the facility to monitor the use of the internet and email. This facility may be used should a manager have reason to believe that the systems are being abused.

16. Physical and Environmental Security

Physical access to high security areas will be controlled with identification authentication techniques and procedures. Staff with authorisation to enter such areas are provided with relevant information on the potential security risks involved in respect of unauthorised access. Physical Security is the responsibility of all employees of the Council. Visitors to any of the Council's offices should not be allowed to wander round at will and should always be accompanied by the visit sponsor.

In addition to general council visitor guidelines, the following must be adopted where individuals are required to administrator access to computer systems i.e. contractors, consultants, third party suppliers, trainers. As opposed to user access to systems i.e. Auditors, bank staff etc.

- ICT Services require a minimum of five working notice in order to prepare for the install, training etc.
- Requests should be made by Systems Administrators and access will need to be co-ordinated with other activities and may not always be achievable.
- Any access to the computer room or telecoms rooms must be accompanied by ICT staff:
- ICT Equipment must be sited in agreement with ICT Staff to ensure adequate ventilation etc.
- Equipment must not be removed or moved to another location without the approval of the ICT Manager.

17. Loss of Equipment or Data

17.1. Equipment / Data Protection Guidelines

The Authority is committed to protecting data, and information held on its computer systems. These guidelines apply to all users of mobile devices whether they are laptops, mobile phones, usb devices or electronic media (CD's), and aim to reduce the risk of sensitive information falling into the public domain.

- Sensitive data stored on laptops and other mobile storage devices should be **kept to a minimum** to reduce risk and impact should a breach of security occur.
- When travelling, equipment (and media) must not be **left unattended** in public places. Portable computers should be carried as hand luggage when travelling.
- When using a laptop, do not process personal or sensitive data in public places e.g. on public transport.
- **Passwords or other access tokens** for access to the Authority's systems should never be stored with or on mobile devices where they may be stolen or permit unauthorised access to information assets.
- Security risks (e.g. of damage, theft) may vary considerably between locations and this should be taken into account when determining the most appropriate security measures.
- It is the employees responsibility to ensure that equipment / devices are reliable, fit for purpose and have the necessary security measures in place.
- Sensitive information held on any mobile device / media must be **securely erased** before the device is reassigned to another user or to another purpose.

17.2. Reporting Equipment / Data Loss

- All incidents of a security nature (loss or theft) should be reported in the first instance to your line manager and ICT.
- All available information should be included - time, location, persons involved, items missing etc.
- An Incident Report Form should be completed as soon as possible after the event by the person reporting the incident and sent to ICT.
- The local Police should be informed in all cases of reported crimes of assault, indecency, fraud, theft and burglary.

18. Suspected Misuse

The Public Interest Disclosure Act 1998 has made it possible for an individual who encounters a malpractice, which could threaten the public interest, to raise his / her concerns without fear of reprisal.

Staff are asked to refer to the Whistle Blowing Policy where they suspect a breach of the ICT Security Policy.

APPENDIX J

Appendices

1. **Acceptable Use Policy**

   SS_POL001

2. **Corporate Policy for the Procurement, Replacement and Configuration of ICT Desktop Equipment**

   SS_POL017