Policy Document

RBC Information Security Policy

Version 3.3

Document Control

Organisation	Redditch Borough Council
Owner	ICT Transformation Manager
Protective Marking	Not protected
Review date	One year from last approval

Revision History

Revision Date	Reviser	Version	Description of Revision
19/02/2013	Mark Hanwell	1.0	Policy created.
2/07/2014	C. Shepard	2.0	Changes to government classification system references
11/12/2015	N Brothwell	3.0	This policy created as a copy of the BDC Information Security Policy v3.0 This Policy also includes the former: • Computer, Telephone and Desk Use Policy • Email Policy • Human Resources Information Security Policy • Information Protection Policy • Internet Acceptable Usage Policy • IT Access Policy • IT Infrastructure Security Policy • Legal Responsibilities • Removable Media Policy • Software Policy • GCSx Policy • Remote Working Policy • Information Security Incident Policy
10/10/2016	N Brothwell	3.1	Access to staff email accounts can be authorised by 4th line managers (changed from HOS).
2/2/2017	M Hanwell	3.2	Password advice updated to include passphrases, and update to passphrase may be annual rather than every 42 days. Also minor update to removable media.
23/03/2017	M Hanwell	3.3	Changes to allow for the use of Drop box for business Cloud storage.

Document Approvals

Sponsor Approval	Name	Date	Version Approved
Head of ICT and Business Transformation	Deborah Poole	19/02/2013	1.0
Head of ICT and Business Transformation	Deborah Poole	12/02/2016	3.0

Head of ICT and Business Transformation	Deborah Poole	23/03/2017	3.3

Document Distribution

This document will be distributed via NetConsent to all Council employees, all temporary staff and all contractors. Councillors will also receive the policies, which they will adhere to when working on behalf of the council. Inform Democratic Services of every policy update.

Contents

1 What is this Policy For?

Throughout this policy, the term 'the Council' refers to Redditch Borough Council.

Information is a major asset. Information security is the protection of information against accidental or malicious disclosure, modification or destruction.

The purpose of this policy is to ensure that the Council protects all information assets within its custody, and that high standards of confidentiality, integrity and availability of information are maintained at all times.

There are seven areas where information security is maintained, and this document is organised into those areas, as follows:

Please refer to the Table of Contents for more details.

2 Who is this Policy for?

This policy applies to all the systems, people and business processes that make up the Council's information systems.

This includes all councillors, committees, departments, partners, employees of the Council, contractual third parties and agents of the Council who have access to information systems or information used for Council purposes.

3 Risks

This policy aims to mitigate the following risks:

- Information being disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance, intentionally or accidentally gaining unauthorised access to business information.
- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities.
- Disclosure of OFFICIAL (all council information is classified as OFFICIAL) or personal or sensitive information as a consequence of loss, theft or careless use.
- Contamination of the Council's networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

4 Information Security – Infrastructure

4.1 Building Security

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have appropriate control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours.
- Window and door locks.
- Window bars on lower floor levels.
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be regularly changed and known only to those people authorised to access the area/building).
- CCTV cameras.
- Staffed reception area.
- Protection against damage - e.g. fire, flood, vandalism.

As an example, access to secure areas such as the data centre and IT equipment rooms must be adequately controlled and physical access to buildings should be restricted to authorised persons. Staff working in secure areas should challenge anyone not wearing a badge. Each department must ensure that doors and windows are properly secured.

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. A Council ICT employee must monitor all visitors accessing secure IT areas at all times.

Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by ICT, as appropriate. Keys are not stored near these secure areas or lockable cabinets.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach. Where breaches do occur, or a member of staff leaves outside normal termination circumstances:

- All identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the staff member
- Door/access codes should be changed immediately.
- Report incident to Information Management team with as much detail as is available, so it can be investigated.

4.2 Equipment Security

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g. if necessary items such as laptops should be physically attached to the desk.

- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs should not have data stored on the local hard drive, nor on the desktop. Data should be stored on the network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an uninterrupted power supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from ICT.

All equipment must have a unique asset number allocated to it. This asset number should be recorded in the departmental and the IS / IT inventories.

For portable computer devices please refer to the 5.13 Remote Working section of this policy.

4.3 Cabling Security

Cables that carry data or support key information services must be protected from interception or damage. Network cables should be protected by conduit and where possible avoid routes through public areas.

4.4 Security of Equipment Off-Premises

The use of equipment off-site must be formally approved by ICT. Equipment taken away from the Council premises is the responsibility of the user and should:

- Be logged in and out, where applicable.
- Not be left unattended.
- Be concealed whilst transported.
- Not be left open to theft or damage whether in the office, during transit or at home.
- Where possible, be disguised (e.g. laptops should be carried in less formal bags).
- Be encrypted.
- Be password protected.
- Be adequately insured.

Users should ensure, where necessary and required, that insurance cover is extended to cover equipment which is used off-site. Users should also ensure that they are aware of and follow the requirements of the insurance policy. Any losses or damage must be reported to the ICT department and the insurance section (if applicable).

Staff should be aware of their responsibilities in regard to data protection and be conversant with the Data Protection Act (please refer to Information Security – Data Protection).

4.5 Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must have all of its data and software erased or destroyed. If the equipment is to be passed onto another organisation (for example, returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools. Equipment must be returned to ICT for data removal.

Software media or services must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

4.6 Delivery and Receipt of Equipment into the Council

In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following guidelines must be applied:

- Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note. Actual assets received must be recorded.
- Loading areas and holding facilities should be adequately secured against unauthorised access and all access should be auditable.
- Subsequent removal of equipment should be via a formal, auditable process.

4.7 Regular Audit

The Council has a duty to audit information security arrangements regularly to provide an independent appraisal and recommend security improvements where necessary.

5 Information Security – Desk, PC, Phone

All of the information the Council handles is designated as OFFICIAL information. This designation is not shown on the information itself. The security of this information is of paramount importance. Information security cannot be achieved by technical means alone; information security must also be enforced and applied by people, and this section addresses security issues related to people.

There is also considerable scope for the misuse of computer resources for fraudulent or illegal purposes, for the pursuance of personal interests or for amusement/entertainment.

Computer and telephony resources include, but are not restricted to, the following:

- Departmental computers.
- PCs.
- Portable laptop computers.
- Printers.
- Network equipment.
- Telecommunications facilities.
- Cameras
- Removable media
- Email
- Internet
- Software

The misuse of the Council's computer and telephony resources is considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action including dismissal.

5.1 Computer Resources Misuse

No exhaustive list can be prepared defining all possible forms of misuse of computer resources; the individual circumstances of each case will need to be taken into account. However, some examples are outlined below:

- Use of computer resources for the purposes of fraud, theft or dishonesty.

- Storing/loading/executing of software that has not been authorised by ICT.
- Storing/loading/executing of software:
    - that has not been acquired through approved Council procurement procedures, or
    - for which the Council does not hold a valid program licence, or
    - that has not been the subject of formal virus checking procedures.
- Storing/processing/printing of data for a purpose which is not work-related.

5.2 Telephone

The Council acknowledges that employees may need to make telephone calls of a personal nature whilst at work. Reasonable steps should be taken by all employees to ensure that the provision of service is not compromised and there is no financial loss.

- Where possible, private calls should be made outside working hours.

- Private calls during these hours should be kept to a minimum, so as not to prevent business calls getting through.

- There may be times when unforeseen working commitments may require the rearranging of personal engagements. The Council recognises that such calls are necessary in order for employees to effectively perform their duties. However, the Council stresses that such calls are normally exceptional, and expect employees to recognise when such calls are required.

5.3 Clear Desk

The Council has a clear desk policy in place in order to ensure that all information is held securely at all times. Work should not be left on desks unattended and should be removed from view when unsupervised.

At the end of each day, every desk will be cleared of all documents that contain any Council information, or any information relating to clients or citizens.

The Council's OFFICIAL information (that is, all council information) must be stored in a facility (e.g. locked safe or cabinet) commensurate with this classification level.

Users of IT facilities are responsible for safeguarding data by ensuring that equipment is locked when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

5.4 Legislation

Users should understand the relevant legislation relating to information security and data protection, and should be aware of their responsibilities under this legislation. The following statutory legislation governs aspects of the Council's information security arrangements. This list is not exhaustive:

- The Freedom of Information Act 2000.
- The Data Protection Act 1998.
- The Computer Misuse Act 1990.

Individuals can be held personally and legally responsible for breaching the provisions of the above and other Acts.

5.5 Storing Data on the Network

All work-related council information should be stored on an appropriate network drive. No data should be stored on the hard drive of a PC or laptop, nor on the desktop.

5.6 Removable Media

It is the council's policy to prohibit the use of all removable media devices except those that are pre-authorised. Requests for access to, and use of, removable media devices such as USB memory sticks, external hard drives, CDs, DVDs and mobile phone storage, must be made to the ICT Helpdesk (ext 1766). You must be able to demonstrate why the use of removable media is the only way for you to carry out council business. The helpdesk will require written permission from your line manager to approve the usage.

Non-Council-owned removable media devices must not be used to store any council information, or used with any council equipment. This means that you must not use your own equipment, for example mobile phones, to store data, for example photographs.

In order to minimise physical risk, loss, theft or electronic corruption, all storage media must be stored in an appropriately secure and safe environment.

All data stored on removable media devices must be encrypted.

Users should be aware that the council will, where possible, audit and log the transfer of data files to and from all removable media devices and council-owned IT equipment – however, it is the responsibility of the user to ensure the removable storage device is encrypted before it is used. ICT can assist with this by a call being raised on the ICT Helpdesk (ext 1766).

5.7 Cloud Storage

The use of Cloud Storage to store any council information needs to be considered very carefully before its use is implemented. In every case, a Privacy Impact Assessment (PIA) should be completed for the subject matter before any document is stored there. Once a PIA has been completed then documents of a none personal nature can be stored using the 'DropBox for Business' cloud storage area. This does not include the DropBox cloud storage used at home or for other personal use as it does not offer the same level of auditing and security that is required by the Council. The use of any other cloud storage is not permitted. For help and advice on cloud storage please contact ICT before using it. There is a license cost for the use of DropBox for business and this will need to be funded by the department wishing to use it.

5.8 Incident Management

It is the duty of all users, including council members, to immediately report any actual or suspected breaches in information security to the ICT Helpdesk (ext 1766).

5.9 Disposing of IT Equipment

IT equipment that is no longer required, or that has become damaged, including software and telephones, must be returned to ICT for disposal.

5.10 Emails

All emails that are used to conduct or support official council business must be sent using a '@bromsgroveandredditch.gov.uk' or '@redditch.gcsx.gov.uk' email address.

Emails held on council equipment are considered to be part of the corporate record and email also provides a record of staff activities. All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

All official external emails must carry the following disclaimer:

*"**********
This e-mail may include confidential information and is solely for the use by the intended recipient(s). If you have received this e-mail in error please notify the sender immediately. You must not disclose, copy, distribute or retain any part of the email message or attachments.*
No responsibility will be assumed by the organisation for any direct or consequential loss, financial or otherwise, damage or inconvenience, or any other obligation or liability incurred by readers relying on information contained in this e-mail or any virus contamination that may occur as a consequence of opening the email or any attachments. Views and opinions expressed by the author are not necessarily those of the organisation nor should they be treated where cited as an authoritative statement of the law and independent legal and other professional advice should be obtained as appropriate.
Any Freedom of Information requests should be sent directly to foi@redditchbc.gov.uk for Redditch Borough Council requests and to foi@bromsgrove.gov.uk for Bromsgrove District Council requests.

**********."

Users should be aware that deletion of email from individual accounts does not necessarily result in permanent deletion from the Council's ICT systems.

It is the responsibility of the person sending the email to decide whether email is the most appropriate method for conveying time-critical or OFFICIAL information (that is, all council information).

If it is necessary to provide a file to another person within the council (that is, with a bromsgroveandredditch.gov.uk email address), then a reference to where the file exists should be sent rather than a copy of the file.

All users should be aware that email usage is monitored and recorded centrally. Monitoring of content will only be undertaken by staff specifically authorised for that purpose within the ICT department. Where a manager suspects that the email facilities are being abused by a user, they should contact their line manager or the ICT Transformation Manager.

Access to another employee's email is forbidden without the express permission of the relevant 4th line manager. If the relevant 4th line manager is not available, then authorisation should be sought from the Head of Service or Director.

Emails sent between '.bromsgroveandredditch.gov.uk' addresses are held within the same network and are deemed secure. Emails sent outside this closed network travel the public communications network and are liable to interception and loss. Therefore, personal or sensitive material must not be sent via email outside a closed network except via GCSx .

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the Data Protection Officer.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council's Equal Opportunities Policy, or which could reasonably be anticipated to be considered inappropriate.

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of the Council's anti-virus software.

5.11 GCSx

GCSx stands for Government Connect Secure Extranet. It is a secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations that sit on the PSN government secure network infrastructure.

Some Council staff will need access to this network in order to carry out their business. This may include staff having access to the secure email facility. All staff requiring access to the GCSx network in any way must be aware of the commitments and security measures surrounding the use of this network, and must have a basic disclosure (DBS) before access is given. This policy must be adhered to by all Councillors, committees, departments, partners, employees of the Council, contractual third parties and agents of the Council using the GCSx facilities.

Each GCSx user must read, understand and accept this policy.

For the avoidance of doubt, the security rules relating to secure e-mail and information systems usage include the following. Please note that all council information is designated OFFICIAL.

1. I acknowledge that my use of the GCSx may be monitored and/or recorded for lawful purposes.

2. I agree to be responsible for any use by me of the GCSx using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and,

3. I will not use a colleague's credentials to access the GCSx and will equally ensure that my credentials are not shared and are protected against misuse; and,

4. I will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and,

5. I will not attempt to access any computer system that I have not been given explicit permission to access; and,

6. I will not attempt to access the GCSx other than from IT equipment and systems and locations which have been explicitly authorised to use for this purpose; and,

7. I will not transmit information via the GCSx that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and,

8. I will not make false claims or denials relating to my use of the GCSx (e.g. falsely denying that an e-mail had been sent or received); and,

9. I will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GCSx to the same level as I would paper copies of similar material; and,

10. I will appropriately label, using the HMG Security Policy Framework (SPF), information up to OFFICIAL sent via the GCSx; and,

11. I will not send sensitive or personal information over public networks such as the Internet; and,

12. I will always check that the recipients of e-mail messages are correct so that potentially sensitive information is not accidentally released into the public domain; and,

13. I will not auto-forward email from my GCSx account to any other non-GCSx email account; and,

14. I will not forward or disclose any sensitive or personal material received via the GCSx unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and,

15. I will seek to prevent inadvertent disclosure of sensitive or OFFICIAL information by avoiding being overlooked by others when I am working, by taking care when printing information received via GCSx (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted; and,

16. I will securely store or destroy any printed material; and,

17. I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via GCSx (this will be in accordance with the Information Security Policy - e.g. logging-off from the computer, activate a password-protected screensaver etc, so as to require a user logon for activation); and,

18. where ICT Services has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection; and,

19. I will make myself familiar with the Council's security policies, procedures and any special instructions that relate to GCSx; and,

20. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security – refer to section 10 Information Security – Data Protection of this policy; and,

21. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and,

22. I will not remove equipment or information from council premises without appropriate approval; and,

23. I will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft) in accordance with section 5.13 Remote Working in this policy; and,

24. I will not introduce viruses, Trojan horses or other malware into the system or GCSx; and,

25. I will not disable anti-virus protection provided at my computer; and,

26. I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs me are relevant.

Document Date:	
Name of User:	
Position:	
Department:	
User Access Request Approved by:	
User Access Request Approved by:	
Username Allocated	
Email Address Allocated:	
User Access Request Processed:	

5.12 Internet Service

The internet service is primarily provided to give Council employees and councillors access to information, research and electronic commerce.

The Council internet should be used in accordance with this policy to access anything in pursuance of your work.

At the discretion of your line manager, and provided it does not interfere with your work, the council permits personal use of the internet in your own time (for example during your lunch break).

The Council is not responsible for any personal transactions you enter in to. You must accept responsibility for, and keep the Council protected against any claims, damages or losses.

5.12.1 Internet Account Management, Security and Monitoring

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted by lack of capacity.
- The filtering system monitors and records all access for reports that are produced for line managers and auditors.

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must **not** use your Internet access to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.

- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter “money making” sites or enter or use “money making” programs.
- Run a private business.
- Download any software that does not comply with section 6 Information Security - Software in this policy.

The above list is neither exclusive nor exhaustive. Unsuitable material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.

You must not attempt to by-pass or remove any of the security and monitoring facilities.

5.13 Remote Working

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

Securing data when users work remotely or beyond the Council network is a pressing issue – particularly in relation to the Council’s need as an organisation to protect data in line with the requirements of the Data Protection Act 1998.

All IT equipment (including portable computer devices) supplied to users is the property of the Council. It must be returned upon the request of the Council. Access for ICT Services staff of the Council shall be given to allow essential maintenance security work or removal, upon request.

All IT equipment will be supplied and installed by Council ICT Service staff . Hardware and software **must only** be provided by the Council.

Where users access Government Connect Secure Extranet (GCSx) type services, facilities or OFFICIAL information (all council information is classified as OFFICIAL), **under no circumstances** should non-Council-owned equipment be used.

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

- Users must take due care and attention of portable computer devices when moving between home and another business site.
- Users will not install or update any software on to a Council-owned portable computer device.
- Users will not install any screen savers on to a Council-owned portable computer device.
- Users will not change the configuration of any Council-owned portable computer device.
- Users will not install any hardware to or inside any Council-owned portable computer device, unless authorised by the Council ICT department.
- Users will allow the installation and maintenance of Council-installed Anti Virus updates immediately.

- Users will inform the ICT Helpdesk (ext 1766) of any Council-owned portable computer device message relating to configuration changes.

- All faults must be reported to the ICT Helpdesk (ext 1766).

- Users must not remove or deface any asset registration number.

- User registration must be requested from the ICT Helpdesk (ext 1766). Users must state which applications they require access to.

- The IT equipment may not be used for personal use by staff. Only software supplied and approved by the Council can be used (e.g. Word, Excel, Adobe, etc.).

- No family members may use the IT equipment. The IT equipment is supplied for the staff members' sole use.

- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, the Council may recover the costs of repair.

- The user should seek advice from the Council before taking any Council supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the Council's normal insurance against loss or theft and the equipment is liable to be confiscated by airport security personnel.

- The Council may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

5.13.1 Remote and Mobile Working Arrangements

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

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use.

Users must ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times. All removable media devices and paper documentation must also not be stored with the portable computer device.

Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing personal data or OFFICIAL information (that is, all council information) must be disposed of in 'confidential waste' bins.

5.13.2 Access Controls

It is essential that access to all OFFICIAL information (that is, all council information) is controlled. This can be done through physical controls, such as locking the home office or locking the

computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all OFFICIAL data (that is, all council information) held on the portable device must be encrypted.

Dual-factor authentication must be used when accessing the Council network and information systems (including Outlook Web Access) remotely via Council owned equipment.

Access to the Internet from Council-owned ICT equipment should only be allowed via onward connection to Council-provided Proxy Servers and not directly to the Internet.

5.13.3 Anti Virus Protection

ICT will deploy an up-to-date Anti Virus signature file to all users who work away from the Council premises. Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least once every two weeks to enable the Anti Virus software to be updated.

5.13.4 User Awareness

The user shall ensure that appropriate security measures are taken to stop unauthorised access to OFFICIAL information (that is, all council information), either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as the Council itself.

5.14 Software

All departments must inform ICT via the ICT Helpdesk (ext 1766) of any new product requirements or of any upgrades, service packs, patches or fixes required to existing systems. All new products must be purchased through ICT.

Every piece of software used by the Council is required to have a licence in the name of the Council. The ICT department maintains a register of all Council software and will keep a library of software licences.

Software is owned by the licencing company and the copying of such software is an offence under the Copyright, Designs and Patents Act 1988, unless authorised by the software manufacturer. It is the responsibility of users to ensure that all software on their computer equipment is licensed.

Software must only be installed by the ICT department once the registration requirements have been met. Software may not be used unless approved by the ICT Manager or their nominated representative.

The Council will ensure that personal firewalls are installed where appropriate. Users must not attempt to disable or reconfigure the personal firewall.

6 Information Security - Software

6.1 Software Acquisition

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

Under no circumstances should personal or unsolicited software (this includes screen savers, games and wallpapers etc.) be loaded onto a Council machine as there is a serious risk of introducing a virus.

6.2 Software Registration

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

Software must be registered in the name of the Council and the department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user.

The ICT department maintains a register of all Council software and will keep a library of software licenses.

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

It is the responsibility of users to ensure that all the software on their computer equipment is licensed.

6.3 Software Installation

Software must only be installed by the ICT department once the registration requirements have been met. Once installed, the original media will be kept in a safe storage area maintained by ICT.

Software may not be used unless approved by the ICT Manager or their nominated representative.

Shareware, freeware and public domain software are bound by the same policies and procedures as all other software. No user may download or install any free or evaluation software onto the Council's systems without prior approval from ICT.

6.4 Personal Computer Equipment

Council computers are Council-owned assets and must be kept both software-legal and virus-free. Only software acquired through the procedures outlined above may be used on Council machines. Users are not permitted to bring software from home (or any other external source) and load it onto Council computers. Council-owned software cannot be taken home and loaded on a user's home computer.

6.5 Software Misuse

The Council will ensure that personal firewalls are installed where appropriate. Users must not attempt to disable or reconfigure the personal firewall software.

It is the responsibility of all Council staff to report any known software misuse to their line manager. Councillors should inform the ICT Manager of such instances.

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

7 Information Security – Access to Software

7.1 Prior to Employment

The Council must ensure that potential users are recruited in line with the Council's recruitment and selection policy for the roles they are considered for and to reduce the risk of theft, fraud or misuse of information or information systems by those users.

7.1.1 User Screening – Potential Employees

Background verification checks must be carried out on all potential users, in accordance with all relevant laws, regulations and ethics. The level of such checks must be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved.

The basic requirements for Council employment are:

- Minimum of two satisfactory references.
- Completeness and accuracy check of employee's application form.
- Confirmation of National Insurance number.
- Confirmation of claimed academic and professional qualifications.
- Identity check against a passport or equivalent document that contains a photograph.

Prospective members of staff who will (if employed) be using the Government Connect Secure Extranet (GCSx) facility must be cleared to Baseline Personnel Security Standard. For this, the following additional requirements must be met:

- Identity must be proven by showing:
  - A full 10 year passport.

  Or two from the following list:
  - British driving licence.
  - P45 form.
  - Birth certificate.
  - Proof of residence – i.e. council tax or utility bill.
- Verification of full employment history for the past 3 years.
- Verification of nationality and immigration status.
- Verification of criminal record (unspent convictions only).

For some jobs a Disclosure and Barring Service (formerly called the Criminal Records Bureau) check on the prospective member of staff must be carried out to an appropriate level as demanded by law.

If the prospective employee would have access to systems processing payment card data, credit checks must be carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

All the above requirements for verification checks must be applied to technical support and temporary staff that have access to those systems or any copies of the contents of those systems (e.g. backup tapes, printouts, test data-sets).

7.1.2 Terms and Conditions of Employment

As part of their contractual obligation users must agree and sign the terms of their employment contract, which shall state their and the Council's responsibilities for information security. This must be drafted by the Council's lawyers and must form an integral part of the contract of employment.

Each user must sign a confidentiality statement that they understand the nature of the information they access, that they will not use the information for unauthorised purposes and that they will return or destroy any information or assets when their employment terminates.

7.1.3 Roles and Responsibilities – New Starters

Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of the information asset owner.

Line managers are responsible for ensuring that creation of new users, changes in role, and termination of users are notified to the ICT Helpdesk (ext 1766) in a timely manner, using an agreed process.

The information security responsibilities of users must be defined and documented and incorporated into induction processes and contracts of employment. As a minimum this will include a statement that every user is aware of, and understands, this policy.

7.2 During Employment

Each user must be allocated access rights and permissions to computer systems and data that:

- Are applicable to the tasks they are expected to perform.
- Have a unique login and password that is not shared with or disclosed to any other user.
- Have individual administrator accounts that will be logged and audited.

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

The unnecessary allocation and use of system privileges significantly increases the vulnerability of systems.

- systems administrative accounts (super users on routers and LAN servers, SANs, etc) must only be used when necessary, and not for normal day-to-day operation;
- Where technically possible, users must initially log on with a personal user ID and only be granted privileged access by way of group assignment;

Administrator accounts should be used only when a standard user account does not have the rights or privileges to perform a task or function required by the corporate demands and should be an extension from within their personal standard account e.g. switch user on Orb from forename.surname to a.initials.

The Council must ensure that all users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their work, and to reduce the risk of human error. It is also necessary that user changes in role or business environment are carried out in an orderly manner that ensures the continuing security of the information systems to which they have access.

7.2.1 Management Responsibilities

Line managers must notify the ICT Helpdesk (1766) in a timely manner of any changes in a user's role or business environment, to ensure that the user's access can be changed as appropriate. Processes must ensure that access to information systems is extended to include new user requirements and also that any access that is no longer needed is removed.

Any changes to user access must be made in a timely manner and be clearly communicated to the user.

Departmental managers must require users to understand and be aware of information security threats and their responsibilities in applying appropriate Council policies. This requirement must be documented.

7.2.2 Information Security Awareness, Education and Training

All users must receive appropriate information security awareness training and regular updates in related statute and organisational policies and procedures as relevant for their role.

It is the role of departmental managers to ensure that their staff are adequately trained and equipped to carry out their role efficiently and securely.

7.2.3 User Responsibilities

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:

- Following the password policy statements outlined in **Error! Reference source not found.**.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing ICT of any changes to their role and access requirements.

7.2.4 User Authentication for Third Parties

Where remote access to the Council network is required, an application must be made via the ICT Helpdesk (ext 1766).

7.2.5 Supplier's Remote Access to the Council Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from the ICT Helpdesk (ext 1766). Any changes to a supplier's

connections must be immediately sent to the ICT so that access can be updated or ceased. All permissions and access methods must be controlled by ICT.

Partners or 3rd party suppliers must contact the ICT Helpdesk (ext 1766) before connecting to the Council network and a log of activity must be maintained. Remote access software must be disabled when not in use.

7.2.6 Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in this section and the **Error! Reference source not found.** section of this policy must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.

All access to operating systems is via a unique login ID that will be audited and can be traced back to each individual user. The login ID must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day-to-day activities.

7.2.7 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The departmental administrator of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with this policy.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

7.3 At the End of Employment

7.3.1 Secure Termination of Employment

Termination of employment may be due to resignation, change of role, suspension or the end of a contract or project. The key requirement is that access to Council information assets is removed in a timely manner when no longer required by the user, and processes must be implemented to ensure this.

7.3.2 Termination Responsibilities

Line managers must notify the ICT Helpdesk (ext 1766) in a timely manner of the impending termination or suspension of employment so that access can be suspended.

ICT Helpdesk (ext 1766) must notify the appropriate system owners who must suspend access for that user at an appropriate time, taking into account the nature of the termination.

Responsibilities for notifying changes, performing employment termination or change of employment must be clearly defined and assigned.

7.3.3 Return of Assets

Processes must be implemented to ensure that users return all of the organisation's assets in their possession upon termination of their employment, contract or agreement. This must include any copies of information in any format.

7.3.4 Removal of Access Rights

If a user's access is considered a risk to the Council or its systems, you must implement emergency suspension of that user's access. Contact Human Resources to ensure the correct procedure is followed.

8 Information Security – Passwords and Passphrases

8.1 Choosing Passwords (or a Passphrase)

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

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

Passphrases are similar to passwords but are longer and made up of several words and with the addition of numbers and possibly other special characters.

For the remainder of this policy the terms password and passphrase are interchangeable.

8.1.1 Weak and strong passwords

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it.

Examples of weak passwords include:

- words picked out of a dictionary
- names of children and pets
- car registration numbers
- simple patterns of letters from a computer keyboard.

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

For this reason when creating or changing your logon account on the Corporate Network, a passphrase is required rather than a single word.

The basic rules of a passphrase are that it needs to be something personal to you, you can remember it without the need to write it down, contains a minimum of 15 characters – at least one of which must be a capital letter and another one a number.

A strong passphrase would be:
MyD4dsNameIsGary – here the passphrase uses a capital letter for the start of each new word and replaces the first letter A with a number 4.

Mydadsnameisgary1– Not as good as the one above but it passes the minimum rules of having minimum 15 characters, one capital letter and one number.

A weak passphrase would be:
Thecowjumpedoverthemoon1 – Whilst this is in accordance with the rules, it is a bare minimum. This is a common phrase and has just one capital letter and one number.

8.2 Protecting Passwords and Passphrases

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

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Council systems.
- Do not use the same password for systems inside and outside of work.
- Avoid writing passwords down. If you must write them down, ensure they are written in code, are not obviously passwords, and do not store them where they are open to theft. Do not store them in electronic documents on your computer.

8.3 Changing Passwords

Given the additional security a good passphrase brings, it needs only be changed once per year, or whenever the system prompts you to change it. Other, shorter passwords, need to be changed every 42 days or when the system prompts you to change it. All default passwords must be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you must change it immediately and report your concern to the ICT helpdesk (ext 1766).

8.4 System Administration Standards

The password administration process for individual Council systems is available to designated individuals.

All Council IT systems will be configured to enforce the following:

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

8.5 PIN Numbers

Users are sometimes given Personal Identification Numbers (PINs), for example to retrieve printouts from a printer.

Users must never reveal PINs to anyone else, and must follow the same security standards as for protecting passwords.

9 Information Security - Asset Management

9.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records.
- Computer databases.
- Data files and folders.
- Software licenses.
- Physical assets (computer equipment and accessories, PDAs, cell phones).
- Key services.
- Key people.
- Intangible assets such as reputation and brand.

The Council must draw up and maintain inventories of all important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information and records management and disaster recovery. At minimum it must include the following:

- Type.
- Location.
- Designated owner.
- Security classification.
- Format.
- Backup.
- Licensing information.

9.2 Classifying Information

On creation, all information assets must be assessed and classified by the owner according to their content. At minimum all information assets must be classified and labelled in accordance with the HMG Security Policy Framework (SPF). The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification. Information classified as OFFICIAL sent via GCSx must be labelled appropriately.

The classes are:

- OFFICIAL
- SECRET
- TOP SECRET

All council information is classified as OFFICIAL.

9.3 Personal Information

Personal information is any information about any living, identifiable individual. The Council is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998.

9.4 Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

9.5 Unclassified Information Assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done.

9.6 Corporate Information Assets

For information assets whose use throughout the Council is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

9.7 Acceptable Use of Information Assets

The Council must document, implement and circulate policies that outline acceptable usage for information assets, systems and services. These should apply to all Council councillors, committees, departments, partners, employees of the Council, contractual third parties and agents of the Council and use of the system must be conditional on acceptance of the appropriate policy. This requirement must be formally agreed and auditable.

9.8 Information Storage

All electronic information will be stored on centralised facilities to allow regular backups to take place. Files which are identified as a potential security risk should only be stored on secure network areas.

ICT services must ensure that guidelines are available for all council staff with regards to identifying redundant equipment and action required e.g. sending to ICT to assess whether it should be disposed of or reused.

Physical files of information should be organised, labelled and managed so that their contents and owners can be identified by other teams, not just the team who owns them.

Records management and retention guidance will be followed for both electronic and physical information. The Retention and Disposal Schedule records how long different types of information should be kept for, it is the responsibility of each team to keep their entries in the Schedule up to date (contact Information Management for more details), and to ensure they are adhered to.

Databases holding personal information will have a defined security and system management procedure for the records and documentation. This documentation will include a clear statement as to the use, or planned use of the personal information.

9.9 Disclosure of Information

Disclosing sensitive or personal information to any external organisation is prohibited, unless via the Government Connect Secure Extranet (GCSx) email. Emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system.

Where information is disclosed or shared it should only be done so in accordance with a documented information-sharing protocol and/or data exchange agreement.

The disclosure of personal or sensitive information in any way other than via GCSx email is a disciplinary offence. If there is suspicion of a Councillor or employee treating OFFICIAL information (that is, council information) in a way that could be harmful to the Council or to the data subject, then it must be reported to the ICT Manager, and the person may be subject to disciplinary procedure.

Any sharing or transfer of Council information with other organisations must comply with all legal, regulatory and Council policy requirements. In particular this must be compliant with the Data Protection Act 2000, The Human Rights Act 2000 and the Common Law of Confidentiality.

10 Information Security – Data Protection

10.1 Relevant Legislation

The following statutory legislation governs aspects of the Council's information security arrangements. This list is not exhaustive:

Legislation	**Areas Covered**
The Freedom of Information Act 2000	Public access to Council information
The Human Rights Act 1998	Right to privacy and confidentiality
The Electronic Communications Act 2000	Cryptography, electronic signatures
The Regulation of Investigatory Powers Act 2000	Hidden surveillance of staff
The Data Protection Act 1998	Protection and use of personal information
The Copyright Designs and Patents Act 1988	Software piracy, music downloads, theft of Council data
The Computer Misuse Act 1990	Hacking and unauthorised access
The Environmental Information Regulations 2004	Public access to Council information related to the environment

Legislation	Areas Covered
The Re-use of Public Sector Information Regulations 2005	The Council's ability to sell certain data sets for commercial gain

Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Key records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

10.2 How will the Council Ensure Compliance?

In order to ensure it meets its obligations under the Data Protection Act, the Council ensures that:

- There is an individual with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Persons wishing to make enquiries about handling personal information, whether a member of staff or a member of the public, is aware of how to make such an enquiry.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.

The Council will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the rights of data subjects can be fully exercised under the Data Protection Act.

10.3 What Roles and Responsibilities have been Assigned?

Proper definitions of roles and responsibilities are essential to assure compliance with this policy. In summary these are as follows:

10.3.1 Information Management Team

The Information Manager promotes this policy and provides detailed advice training and resources to departments to facilitate the correct processing of requests for access and other data protection related issues, and will also monitor departments to ensure compliance with statutory and regulatory obligations.

10.3.2 Senior Management

Senior management will provide support and approval for this Information Security Policy and any related initiatives across the Council. It will also ensure that adequate funding is made available.

10.3.3 Departmental Managers

Departmental managers are responsible for ensuring that the Information Security Policy is communicated and implemented within their area of responsibility, and for ensuring that any issues such as resourcing or funding are communicated back to their strategic directors in a timely manner.

10.3.4 Individual Employees

Individual employees will be responsible for understanding this Information Security Policy and ensuring that requests for access and other data protection related issues in their own department are handled in compliance with this policy.

10.4 Freedom of Information Act

The Freedom of Information Act came into force in January 2005. By granting a general right of access to records held by public authorities it encourages an attitude of openness and will enable the public to scrutinise their decisions and working practises. The key features of the Freedom of Information Act are:

- Every Council employee has a duty to provide advice and assistance to anyone requesting information.
- The public has a general right of access to all recorded information held by the Council and some independent contractors. Subject to exemptions set out in the Freedom of Information Act, a requester has the right to know whether a record exists and the right to a copy of that record supplied in a format of their choice.
- Every Council must adopt and maintain a Publication Scheme, listing what kinds of record it chooses to publish, how to obtain them and whether there is a charge involved.

The Information Commissioner's Office will oversee the implementation and compliance with the Freedom of Information Act and the Data Protection Act 1998.

10.5 What is a Security Incident?

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the Information Management team. It is vital for the Information Management team to gain as much information as possible from the business users to identify if an incident is occurring.

The definition of an information management security incident is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An information security incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

Examples of the most common information security incidents are listed below. This list is not exhaustive.

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Infecting a computer with a virus or other malware.
- Sending a sensitive email to 'all staff'.
- Receiving solicited mail of an offensive nature.
- Receiving solicited mail which requires you to enter personal data.
- Changing data without authorisation.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others other than the ICT helpdesk (ext 1766).
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).
- Use of unapproved or unlicensed software on Council equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.
- Theft / loss of a hard copy file through negligence.
- Theft / loss of any Council computer equipment e.g. laptops, memory sticks and CDs through negligence.

This policy aims to ensure incidents are followed up correctly, and to identify areas for improvement to decrease the risk and impact of future incidents.

10.5.1 Procedure for Incident Handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the Information Management team. It is vital for the Information Management team to gain as much information as possible from the business users to identify if an incident is occurring.

1. Report incident to Information Management team with as much detail as is available.
2. Report incident to line manager. Emergency suspension of a user's access may be necessary if that access is considered a risk to the Council or its systems.
3. Information Management team will assess incident against the ICO data breach guidance, to decide whether to report the incident to the ICO.
4. Information Management team will assess incident and decide on actions to be taken.

The Information Management team will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information should be supplied:

- Contact name and number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

The authority may need to collect evidence. This could include, for example, personal information, deleted files, and emails from any asset owned by the Council.

10.6 Individual Responsibilities

All Councillors must accept responsibility for maintaining information security standards within the Council.

All managers must accept responsibility for initiating, implementing and maintaining security standards within the Council.

All non-managerial users must accept responsibility for maintaining standards by conforming to those controls which are applicable to them.

ICT will be responsible for implementation of the controls marked for IT specialists.

Local managers must undertake yearly assessments of security risks within their own areas to ensure that the security breaches are kept to a minimum.

11 Key Messages

Access:

- Every user must be aware of, and understand, this policy.
- Background verification checks must be carried out on all users.
- Users who require use of the Government Connect Secure Extranet (GCSx) email facility **must** be cleared to Baseline Personnel Security Standard.
- All users must receive appropriate information security awareness training and regular updates in related statute and organisational policies and procedures as relevant for their role.
- Processes must be implemented to ensure that all access rights of users of Council information systems shall be removed in a timely manner upon termination or suspension of their employment, contract or agreement.

Information Protection:

- The Council must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG Security Policy Framework (SPF).
- Information classed as OFFICIAL (that is, all council information) sent via the Government Connect Secure Extranet (GCSx) must be labelled appropriately using the SPF guidance.
- Access to information assets, systems and services must be conditional on acceptance of the appropriate policy.
- Users should not be allowed to access information until they understand and agree the legislated responsibilities for the information that they will be handling.
- Personal or sensitive information **must not** be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing personal or sensitive information to any external organisation is also **prohibited**, unless via the GCSx email.
- Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating personal or sensitive material.
- The disclosure of personal or sensitive information in any way other than via GCSx email is a disciplinary offence.

IT Access

- All users must use **strong** passwords.

- Passwords must be protected at all times and must be changed at least every 42 days.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from the ICT Helpdesk (ext 1766).
- Partners or 3rd party suppliers must contact the ICT Helpdesk (ext 1766) before connecting to the Council network.

IT Infrastructure Security

- OFFICIAL information (that is, all council information), and equipment used to store and process this information, must be stored securely.
- Keys to all secure areas housing ICT equipment and lockable IT cabinets are held centrally by ICT, as appropriate. Keys are not stored near these secure areas or lockable cabinets.
- All general computer equipment must be located in suitable physical locations.
- Desktop PCs should not have data stored on the local hard drive.
- Non-electronic information must be assigned an owner and a classification.
- Staff should be aware of their responsibilities in regard to the Data Protection Act.
- Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed.

Software

- All software acquired must be purchased through the ICT Department.
- Under no circumstances should personal or unsolicited software be loaded onto a Council machine.
- Every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.
- Unauthorised changes to software **must not** be made.
- Users are not permitted to bring software from home (or any other external source e.g. ipod, mobile phone, personal memory stick, email) and load it onto Council computers.
- Users **must not** attempt to disable or reconfigure the Personal Firewall software.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

Remote Working

- It is the user's responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention when moving portable computer devices and not emailing personal or sensitive information to a non-Council email address.
- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- It is the user's responsibility to ensure that access to all OFFICIAL information (that is, all council information) is controlled – e.g. through password controls.
- All council data held on portable computer devices must be encrypted.

Information Security Incident

- All staff should report any incidents or suspected incidents immediately by reporting them to the Information Management team
- We can maintain your anonymity when reporting an incident if you wish.