South Cambridgeshire District Council

ICT Security policy and usage guidelines

2010/11

Changes from previous (May 2010)

Date of review:	1st October 2010
Next review date:	1st April 2011
Document status:	Live

Section Two

Computer Security Policy

1. Introduction

This section is intended for all users and relates to the general use and security of ICT equipment. It includes:

Sub-section	***Subject Area***
System Access Policies	Controls relating to user access of computer equipment, such as passwords.
Information Policies	Policies to protect the confidentiality and integrity of the Council's data.
Software Policies	Policies to protect the integrity, appropriateness and legality of the Council's software packages.
Computer Hardware/Physical Systems Policies	Policies and guidelines to protect ICT hardware against potential damage (either to the hardware or to staff) or theft.

The Council has agreed the policies and guidelines. Failure to comply with the policies and guidelines will be considered a serious offence and may lead to disciplinary procedures.

2. System Access Policies

Number	***Policy Item***
1.	You should only access information that is your own, that is publicly available, or that to which you have been given authorised access.
2.	Never use or borrow a colleague's user name or password or allow anyone to borrow yours. If you have forgotten your user name or password, contact the Help Desk (x3400). Violation of this access policy will be considered a disciplinary offence.
3.	All users must have 'strong' passwords. Passwords must be alphanumeric, have a minimum of 7 characters in length and contain at least one digit. It is the user's responsibility to prevent their user ID and password being used to gain unauthorized access to Council systems. Change your passwords if you have any reason to believe that someone else knows them.
4.	Passwords must not be written down in a way that can be interpreted by someone else.
5.	Always protect your password.
6.	Network access passwords will be changed every 60 days. You will receive automatic reminders to do this. Password history protection disables your ability to 'recycle' recently used passwords.
7.	When accessing non-work related Internet sites, never use a South Cambridgeshire District Council password or User ID to register a login.

Number	*Policy Item*
8.	Always log out, shut down or "lock" your computer when it is unattended (particularly at lunchtime and during meetings). PC's will automatically lock if left unattended for more than 10 minutes. Alternatively, you can lock your PC by pressing Ctrl, Alt, Delete at the same time, then clicking on "Lock Computer". Unless you have special requirements authorised by the ICT Support Services Manager or Head of ICT, you should shut down your computer at the end of the working day. (NB. Always do this before switching it off). In the event that computers are not shut down, automated systems will be employed to enforce energy savings requirement.
9.	Managers must ensure that access rights to systems are removed when users leave Council employment, or such access rights are modified appropriately when users move to a different job function. This should be instigated by providing details to the Help Desk (x3400) in advance of the change in status.
10.	Managers / HR must ensure that the Help Desk (x3400) is informed of any new starters in order for them to be registered on the appropriate systems and if necessary additional equipment ordered.
~~11.~~	~~In all cases, unless there is a technical exception that cannot be overcome, all remote access to SCDC systems will be facilitated by correctly authenticated 2 factor SSL-VPN sessions. Only under exceptional circumstances will modems used by third parties to access systems. Any such modems must be disabled or disconnected at all times except when legitimately required. The process by which a third party will access the system will be managed by the ICT Support Team.~~
11.	In all cases, unless there is a technical exception that cannot be overcome, all remote access to SCDC systems will be facilitated by correctly authenticated 2 factor SSL-VPN sessions. Access to Councils network and systems from internet cafes or other 'untrusted' environments is strictly forbidden, any such actions could result in disciplinary proceedings. Only under exceptional circumstances will modems used by third parties to access systems. Any such modems must be disabled or disconnected at all times except when legitimately required. The process by which a third party will access the system will be managed by the ICT Support Team.

3. Information Policies

Number	*Policy Item*
1.	ICT will ensure appropriate controls and procedures are established to protect the security of data on networks, and the protection of connected services from unauthorised access.
~~2.~~	~~Anti-virus checks should be done routinely on all software, disks and systems. All South Cambridgeshire District Council PCs and Laptops have SOPHOS Antivirus (automatic virus checking software) installed; it is an offence to change the installed setting as this could interfere with its accuracy of virus detection. Any item found to be infected must be reported immediately to the Help Desk (x3400). Computers and/or laptops used to remotely access Council systems should be updated with the latest antivirus software, operating system releases, security patches and application software releases. NAC (network access control) will be used to quarantine any device found not to meet the Councils security standards.~~
2.	Anti-virus checks should be done routinely on all software, disks and systems. All South Cambridgeshire District Council PCs and Laptops have SOPHOS Antivirus (automatic virus checking software) installed; it is an offence to change the installed setting as this could interfere with its accuracy of virus detection. Any item found to be infected must be reported immediately to the Help Desk (x3400). Computers and/or laptops used to remotely access Council systems should be updated with the latest antivirus software, operating system releases, security patches and application software releases. NAC (network access control) will be used to quarantine any device found not to meet the Councils security standards. Access to Councils network and systems from internet cafes or other 'untrusted' environments is strictly forbidden, any such actions could result in disciplinary proceedings
3.	You must inform the Senior Information Management Officer of all new databases created that will be used to store personal data.

Number	Policy Item
4.	If there is any doubt relating to the source or content of information, seek advice from the Help Desk (x3400) before opening or saving the file.
5.	Reasonable precautions must be taken when transferring personal / sensitive data in either hardcopy or electronic form. Always ensure sensitive information to which you have access is used securely and is only disclosed to those users who are authorised to have access to it. For example, always destroy printed output of a sensitive nature. Confidential output must be placed in a secure confidential waste bin or shredded.
~~6.~~	~~Ensure that personal / sensitive data is transferred under conditions of security appropriate to the type of data and anticipated risk. Employees are responsible for:~~ ~~oThe security of any data they extract or otherwise remove from Council owned systems~~ ~~oThe security of any data they place on personally owned or Council owned computers being used from remote locations.~~ ~~Sensitive data should never be transmitted via email or in any other plain text or common format. ICT Support can assist with secure, encrypted transmission of sensitive data.~~
6.	Ensure that personal / sensitive data is transferred under conditions of security appropriate to the type of data and anticipated risk. Employees are responsible for: o The security of any data they extract or otherwise remove from Council owned systems o The security of any data they place on personally owned or Council owned computers being used from remote locations. Access to Councils network and systems from internet cafes or other 'untrusted' environments is strictly forbidden, any such actions could result in disciplinary proceedings Sensitive data should never be transmitted via email or in any other plain text or common format. ICT Support can assist with secure, encrypted transmission of sensitive data.
7.	Sensitive computer data should be stored in the shared folders on servers provided by ICT, such as the W, X and Y drive. This will ensure the security of the data copy and that regular backups are taken. You should only store personal data locally on your PC hard drives with your manager's permission, and in this case you are responsible for taking back-ups and storing them securely. Use of the Z drive should be restricted to personal confidential matter, do not use the Z drive to store documents to be shared / accessed by colleagues.
8.	Avoid copying or downloading sensitive data from the Councils systems to your PC, PDA, Laptop etc unless absolutely required. Controls to protect the sensitivity of Council data may not be available on other systems or devices. In all cases, you should ensure you have the appropriate permissions.

4. Software Policies

Number	Policy Item
1.	If you believe that you have a computer virus, or you receive an email relating to a computer virus, contact the Help Desk (x3400) immediately.
2.	No user should make or use unlicensed or illegal copies of copyrighted software under any circumstances. Users are not permitted to bring software from home (or any other external source) and load it onto Council computers. Under no circumstances should personal or unsolicited software be loaded onto a Council machine
3.	Never intentionally access or transmit computer viruses, malware, adware or similar software.
4.	All new software should be checked and installed by ICT, unless agreed otherwise with the ICT Support Services Manager or Head of ICT. 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

Number	*Policy Item*
5.	Any software not installed and/or supported by ICT which: ○ Causes a technical problem ○ Is being used illegally ○ Is found to be offensive or inappropriate ○ Contravenes ICT Strategy requirements ○ Is otherwise considered to be a security risk may be removed from your PC and/or the standard corporate PC 'image' will be restored.
6.	Unauthorised users should not access, copy, alter, or interfere with computer programs or data. Unauthorised changes to software must not be made.
7.	Staff negotiating contracts under which software is to be written for the Council must ensure that suitable arrangements are made for the copyright to be vested in the Council. If appropriate, line of business applications should be considered for ESCROW status.
8.	Users must not attempt to disable or reconfigure any computer system security software including the Councils Anti Virus or Personal Firewall software.

5. Computer Hardware/Physical Systems Policies

Number	*Policy Item*
1.	Always take appropriate steps to ensure the security of South Cambridgeshire District Council hardware when away from the premises. For example, never leave computer equipment (PARTICULARLY LAPTOPS) in your vehicle, hidden from view or not. Security of the equipment is the users responsibility.
2.	Personal computers should, where possible and appropriate, be sited away from windows and doors; if appropriate, the equipment should be secured to furniture to reduce the likelihood of theft.
3.	Where systems and/or equipment are made available to you for use outside of normal South Cambridgeshire District Council office locations, then all the policies here will apply.
4.	Access to peripheral devices with memory storage capabilities will be controlled to ensure appropriate security of sensitive data. Devices such as writeable CD's, PDA's, digital cameras etc will only be allowed access to the Councils systems after authorisation by the ICT Support Services Manager and / or the Head of ICT. The Councils systems will only allow access to council owned and encrypted USB memory devices, all other such devices will be refused access.
5.	All equipment should be identified via a secure label ("asset tag") and included in the Council's inventory list maintained by ICT. Users should report any deliveries of ICT equipment and other related hardware to ICT so that such marking can take place. Users should report to the Help Desk (x3400) any equipment that is not asset tagged.
6.	ICT must ensure that all ICT hardware complies with Health & Safety regulations. All users are required to co-operate with ICT staff in their efforts to ensure Health & Safety regulations are being met.
7.	Unless specifically authorised by the Head of ICT, you should not connect non-South Cambridgeshire District Council hardware to the network. In exceptional circumstances, where connection to the network is to be allowed, this will only be permitted once the hardware in question has been subjected to the appropriate anti-virus health checks and verified as clean and safe.

Number	*Policy Item*
8.	Do not install modems on South Cambridgeshire District Council PCs or laptops. If a modem is required, the request needs to be authorised by the ICT Support Services Manager and / or Head of ICT.
9.	When leaving the employment of the Council, all manuals, equipment, documentation and any other materials belonging to the Council must be returned on or before your last working day.
10.	Information Technology facilities and equipment supporting critical or sensitive business activities must be housed in secure areas and physically protected from security threats and environmental hazards. The Council has provided a secure ICT Computer Room managed by the ICT Support team for this purpose. Where it is not practicable to locate equipment in the ICT Computer Room, please contact the Help Desk (x3400) for advice on secure equipment location.
11.	Any potential security problems relating to computer hardware should be reported to the Help Desk.
12.	Wherever practicable output devices, such as printers, should be located where they are readily visible to the person who requested the output, so that sensitive data can be collected immediately. When using corporate multi-functional printing devices, users should use the appropriate password protection to ensure the confidentiality of sensitive data.

6. Government Connect Secure Extranet (GCSx) Policies

Number	*Policy Item*
For nominated users of the Government Connect Secure Extranet (GCSX), In addition to the policies contained within this document, the GCSx network requires:	
1.	All users of the GCSx connection must be aware of the commitments and security measures surrounding the use of this network. All Councillors, Committees, Services, Partners, Employees of the Council, contractual third parties and agents of the Council using the GCSx facilities, must adhere to this policy. All users requiring access to the GCSx network in any way will be required to: ○ Read and understand the GCSx Acceptable Usage Policy (AUP) and sign the Personal Commitment Statement. ○ Understand that any communication sent via GSI / GCSx may be intercepted or monitored. ○ Agree to comply with all of the Councils security rules and associated ICT Security Policies and Usage Guidelines

2.	Users of the GCSx will take all reasonable precautions to prevent the unauthorized disclosure of Sensitive, PROTECTED or RESTRICTED information. Users will follow the Councils Information Protection Policy for processing records and information, which are protectively marked; understand the risks of disclosing PROTECTED or RESTRICTED records and information via unsecure communication methods; the impact and actions to be taken in the event of data loss. o All information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG Security Policy Framework (SPF). o Information up to RESTRICTED sent via the Government Connect Secure Extranet (GCSx) must be labelled appropriately. o Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy (AUP). o PROTECT and RESTRICTED information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone. O Disclosing PROTECT or RESTRICTED classified information to any external organisation is also prohibited, unless via the GCSx email. o 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 PROTECT or RESTRICTED material. O The disclosure of PROTECT or RESTRICTED classified information in any way other than via GCSx email will be considered a disciplinary offence.
3.	All information security events or incidents must be reported immediately to the ICT Helpdesk to ensure timely investigation, response and action. ICT Helpdesk will escalate to the Head of ICT where appropriate. An Information Security Incident includes, but is not restricted to: o The loss or theft of data or information o The transfer of data or information to those who are not entitled to receive that information o Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system o Changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent o Unwanted disruption or denial of service to a system o The unauthorised use of a system for the processing or storage of data by any person Where appropriate, ICT will report the incident to the Computer Emergency Response Team at GovCert.UK for action/follow-up.

4.	Security scanning will take place on a regular basis and at least: ○ On a quarterly basis, network scanning will be conducted to ensure a safe and compliant infrastructure. ○ On an annual basis, ICT will carry out an IT Health Check as part of the annual Government Secure Intranet re-authorisation submission. ○ Users will be required to participate in the testing.
5.	Users of the GCSX network will be allocated a unique user ID. All users must have strong passwords, which must be protected at all times. Passwords must be alphanumeric, have a minimum of 7 characters in length and contain at least one digit. It is the user's responsibility to prevent their user ID and password being used to gain unauthorized access to Council systems. ○ Passwords must be protected at all times and must be changed at least every 60 days. Password history prevents recycling of existing passwords. ○ User access rights will be reviewed at regular intervals ○ Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from ICT Helpdesk ○ Partners or 3rd party suppliers must contact the ICT Helpdesk before connecting to the Councils network
6.	If mobile services are accessed from outside the United Kingdom then users must follow the instructions given by ICT and understand the risks of using IT equipment abroad.
~~7.~~	~~Mobile and/or remote working solutions must be via Council approved means..~~
7.	Mobile and/or remote working solutions must be via Council approved means. .Access to Councils network and systems from internet cafes or other 'untrusted' environments is strictly forbidden, any such actions could result in disciplinary proceedings.
8.	All user activities will be logged and will be reviewed by Management and Gov Connect as required.
9.	Users must not copy sensitive data onto personal portable media devices, always ensure a Council owned device is used. PC's will be configured to restrict access to unauthorised devices.
10.	Protectively marked email information must only be sent via the GSi network. Protected information must not be sent or forwarded to personal email accounts or less secure domains.
11.	Users must ensure that appropriate security measures are taken to stop unauthorised access to PROTECTED or RESTRICTED information, either on portable computer devices or in printed format. Confidentiality and Data Protection principles apply.

13.	It is the Councils policy to manage the use of all removable media devices. The use of removable media devices will only be approved if there is a valid business case for its use. All use of removable media / removable media devices is monitored, all content on removable media / removable media devices is checked for integrity. o Any removable media device that has not been supplied by ICT must not be connected to Council equipment or the Councils network. o All data stored on removable media devices must be encrypted where possible. o Damaged or faulty removable media devices must not be used. Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss Removable media devices that are no longer required, or have become damaged, must be returned to ICT to be disposed of securely to avoid data leakage.
14.	The Council and its users must adhere to all current and future legislation relating to data/information sharing, manipulation and copying. o The Council will ensure compliance with the Data Protection Act 1998 o Staff should be aware of their responsibilities in regard to the Data Protection Act. o The Council has established a number of roles to assure compliance of this policy o Every Council user has a duty to provide advice and assistance to anyone requesting information under the Freedom of Information Act o All Councilors must accept responsibility for maintaining Information Security standards within the Council o PROTECT or RESTRICTED information, and equipment used to store and process this information, must be stored securely. o Desktop PCs should not have data stored on the local hard drive. O Non-electronic information must be assigned an owner and a classification. PROTECT or RESTRICTED information must have appropriate information security controls in place to protect it.