Internet and Email Policies

Any access to the corporate internet and email facilities must be via Council supplied hardware and software, a signed usage agreement is required.

Monitoring of the internet and email usage via these facilities can take place to ensure it is not being misused.

All e-mail received by or sent from the Council's systems will be retained by the Council's archive system and will be available for retrieval at a later date should this be required.

When working at South Cambs Hall, web content filtering and blocking facilities will be used to prevent access to unauthorised or inappropriate content.

You should not use the Council's facilities for political lobbying.

Never give out your Council email address to a website.

Do not download software (including games and screensavers) from the internet. If you have a specific requirement contact the HelpDesk on 01954 713400 or by email (helpdesk@scambs.gov.uk).

You must not at any time use, display or transmit material which is obscene, sexually explicit, pornographic, racist, defamatory, depicts criminal or terrorist acts or could be described as objectionable in any other way.

Email (incoming and outgoing) must be treated in the same way as other formal correspondence. Where possible, do not send highly confidential material via email unless it can be encrypted or password protected.

Unless specifically authorised, do not attempt to access another user's email or internet facilities.

Avoid sending email with large attachments (>5Mb)

Do not open email from untrusted sources.

Do not represent your personal opinions as those of the Council.

Remember……..

The Council's facilities are primarily for the conducting of Council business.

Responsible personal use is allowed.

Inappropriate use of the internet or email will be considered a disciplinary offence and may lead to dismissal. It could also lead to criminal or civil action if legislation is contravened.

It is your responsibility to comply with the ICT Security Policy and Usage Guidelines.

Don't be afraid to ask! If you think you have a legitimate business need to access a function, service or area of the internet which has been barred/ removed, please contact Democratic Services or the Head of ICT to discuss the options available.

For more in-depth information including the web filter and email filter settings, the full document is available on the Council's intranet at:

http://InSite/PoliciesStrategiesProcedures

Your quick and easy guide to all you need to know about computer security as a Member

For more information about the ICT Security Policy and Usage Guidelines contact:

Steve Rayment
Head of ICT
Extension 3010
email: steve.rayment@scambs.gov.uk

April 2011

South Cambridgeshire District Council

ICT Security Policy and Usage Guidelines April 2011

Your quick and easy guide to all you need to know about computer security as a Member

Why have an ICT Security Policy?

In today's modern world more and more of the Council's business is being conducted electronically . The Council has a responsibility to ensure the availability, integrity and confidentiality of its systems and data. The recent increases in the use of the internet and email has placed further demands on those systems.

The ICT Security Policy and Usage Guidelines exist to protect both the Council, its staff and Members. This leaflet is designed to help guide you through the important issues covered in that document.

In addition to our own Council policies, we need to ensure that IT legislation is adhered to and this includes:

Electronic Communications Act 2000
Regulation of Investigatory Powers Act 2000
Telecommunications (Fraud) Act 1997
Computer Misuse Act 1990 (c.18)
Copyright, Designs and Patents Act 1988
Environmental Information Regulations 2004
Freedom of Information Act 2000
Data Protection Act 1998
please note: The DPA also applies to any paper filing systems

This policy applies to all onsite, offsite, desktop and portable hardware and software, which may or may not be provided by the Council but is used for the conducting of Council business as agreed in the 'user agreement'. Any breach of this legislation may result in further investigation and appropriate action.

It is your responsibility to ensure you are fully aware of the policy and its contents.

The Rights of the Council

The Council reserves the right to monitor and / or log all uses of the internet, intranet and email systems from its premises and if required, access any email or email account.

For Council owned equipment, it reserves to right to request sight of the equipment and carry out appropriate checks for inventory (hardware and software) as may be required from time to time.

The Council reserves the right to:

Withdraw access to any computer systems and services.

Prohibit access to certain webpage's, areas of the internet and other internet resources.

Computer Security

Common sense and the adherence to some fundamental principles form the backbone of Computer Security and is encompassed in 4 main areas.

System Access
You should only access systems and information that you have been authorised to do.

Never allow another user/member to have access to your passwords.

Do not write your password down and always protect it.

Always log out, shut down or lock your computer when unattended. Ensure all dialup modems are disconnected when not in use.

Do not connect any non-SCDC provided equipment to the councils network.

Information Policies
Always ensure sensitive and/or confidential information to which you have access is used securely and is not disclosed to unauthorised users.

Always inform the Senior Information Management Officer of any new databases that store personal data.

Always keep the data in a secure manner. The most common used location on the PC / Laptop is 'My Documents' - remember that all such data is vulnerable to possible loss; if you have important information, please ensure you create a backup copy.

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

Software Policies
Never download or copy unlicensed or illegal copies of software under any circumstances.

Never install any software on Council owned equipment without proper authorisation and preferably, always ask ICT support to carry out the installation for you.

The Council reserves the right to remove any software from it's equipment, which is not authorised or is found to be inappropriate or the cause of technical issues.

Computer Hardware/Physical Systems Policies
Always take reasonable steps to ensure the physical security of Council provided equipment.

Do not leave equipment in full view and where appropriate, keep away from windows, doors etc.

If you are using equipment provided by the Council, regardless of location, all policies will apply.

All Council provided equipment is to be asset tagged and identified as belonging to the Council.