South
Cambridgeshire
District Council

ICT Security policy and usage guidelines

2006/2007

Date of creation:	5th June 2006
Review date:	16th June 2006
Next review date:	31st March 2007
Document status:	Draft Version 3

Foreword

Computers are central to the operation of the Council and the increasing importance of the use of electronic information not only internally with the Council but for ‘citizen-centric’ and ‘business to business’ communication highlights the need to understand how this technology exposes the Council to legal liability.

The ease of use of email (quick, effective, cheap) encourages the adoption of a more relaxed manner. It is seen as more akin to a verbal form of communication (telephone) rather than a formal typed letter. However, it is important to realise that emails produce an evidential record. Employees may give less thought to an email than a formal typed letter/memo and thus may state comments that could eventually be used in support or in defence of an organisation’s legal position in the event of a dispute. Emails are not private, they are the most exposed form of communication.

In addition, it is difficult to ascertain the tone of the email message and therefore bullying and intimidating reprimands through this medium may lead to stress or personal injury claims.

At the touch of a button, emails can be sent immediately anywhere in the world or to too many people – at best it could lead the sender to make an embarrassing apology or at worst it could become the basis of a lawsuit in Court.

It is also worth remembering the Internet is not secure. There is a risk that information provided over the Internet might be intercepted by people you wouldn't want to read it. Information you provide to a website may be made available anywhere in the world and may not be protected by data protection legislation.

The objective of this document is to emphasise the importance of access and use of ICT facilities such as the Internet and email and to protect the privacy and legal interests of the Council, its employees, and its customers.

The approach used in this document is to encourage you to consider a series of issues about the usage and environment of ICT systems. For ease of use, the document is split into several sections. Please ensure you are familiar with the policy and it’s implications; if in doubt, please ask.

Steve Rayment

Assistant Director (ICT)

Table of Contents

Version Control

Version Number	Date	Revision Details	Updated by
Draft version 1	*April 2001*	*Initial draft*	*Mark Garvey (LDA)*
Draft version 1.1	*March 2002*	*Update to Sections 2 & 3.*	*Paul Barnes*
Draft version 1.2	*May 2002*	*Section 5 & 6 added. Appendices 1, 2 & 3 added.*	*Paul Barnes*
Draft version 2	*June 2002*	*General review and update*	*Malcolm Wylie*
Draft version 2.1	*August 2002*	*Update following review by Legal and HR*	*Malcolm Wylie*
Final version 1	*October 2002*	*Consolidated into one document, and a minor change to the email disclaimer*	*Malcolm Wylie*
Final version 2	*July 2003*	*Email filter settings*	*Steve Rayment*
Revison – version 3.1	April 2006	General review and update. Removal of ITNET references	Steve Rayment
Revision – version 3.2	May 2006	Update for email and web filtering systems	Steve Rayment
Draft version 3	June 2006	Updated to include current position and infrastructure changes	Steve Rayment

Section One

ICT Security Policy & Guidelines Introduction

1. Introduction

An effective level of computer security, based on risk and exposure, is required within the Council to ensure that the confidentiality, availability and integrity of computer systems is established and maintained. This has become particularly important with the Internet and Email accessibility provided by the Council.

The summarised guidelines in this section should be read by everyone and continually referenced to provide the reader with a complete picture of the Council's minimum computer security requirements.

This policy has the full support of the Members and Management Team of South Cambridgeshire District Council.

2. Guidance

The ICT Team will provide advice and guidance on all aspects of ICT security, including any questions on this document. If you suspect there has been a security breach, you should contact the Helpdesk immediately (x3400).

3. IT Legislation

You must adhere to current and future legislation relating to data/information sharing, manipulation and copying. This includes

Electronic Communications Act 2000

- An Act to make provision to facilitate the use of electronic communications and electronic data storage
- An electronic signature shall be admissible in evidence

Telecommunications (Fraud) Act 1997

- An Act to amend the Telecommunications Act 1984 to make further provision for the prevention of fraud in connection with use of a telecommunication system.

Computer Misuse Act 1990 (c. 18)

- Unauthorised access to programs and data.
- Unauthorised access with intent to commit a crime.
- Unauthorised modification of contents (this includes introducing viruses).

Computer Copyright Act 1988

- Under this law, a piece of software is regarded as the intellectual property of the person who wrote it, or the organisation, which employed the person to write it.

Data Protection Act 1998

Personal data should:

- be held for specific purposes
- be obtained and processed fairly and lawfully
- be adequate, relevant and not more than is required for the specific purpose
- be accurate and kept up-to-date

Personal data should not:

- be disclosed or used in any manner which is incompatible with the specific purpose for which it was obtained
- be held any longer than necessary

A breach of this legislation may result in disciplinary action. These guidelines apply to all onsite, offsite, desktop and portable hardware and software (as well as paper filing systems).

Freedom of Information Act 2000

The Freedom of Information Act applies to all 'public authorities' - this includes:

- central and local government
- the health service
- schools, colleges and universities
- the police
- lots of other non-departmental public bodies, committees and advisory bodies.

The FOI Act was passed to make a major step forwards in terms of openness and accountability and is part of a wider group of policies and gives any person the legal right to ask for and be given any information which is held by a public authority .

4. The Rights of the Council

South Cambridgeshire District Council reserves the right to monitor and/or log all uses of the Internet, email, and the Intranet.

All information sent via email remains the property of South Cambridgeshire District Council and may not be considered the property of the private individual.

The Council reserves the right to:

- Withdraw users' access to any computer systems and communication services, including Internet services
- Prohibit access to certain specific newsgroups, web pages and other Internet resources
- Remove or substitute the hardware or software used to access the Internet at any time and for any reason.

5. Roles and Responsibilities

For this policy to be effective everybody must take personal responsibility for security, in particular Directors and Managers should be vigilant. The responsibility for the maintenance and updating of this policy lies with the Assistant Director (ICT). User interests are reflected through the Service Users Meeting with IT Group (SUMIT).

6. Enforcement

South Cambridgeshire District Council considers any violation of the policies set out to be a serious offence. All breaches of the policy will be investigated by the Human Resources section in-conjunction with Legal, Audit and ICT. Any action taken will be in accordance with the relevant disciplinary procedure.

Section Two

Computer Security Policy

1. Introduction

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

Sub-section	***Subject Area***
System Access Policies	Controls relating to staff 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 policies and guidelines have been agreed by the Council at Chief Officer level. 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).
3.	Select passwords that are a minimum of six characters in length, which are not easily guessed, and change your passwords if you have any reason to believe that they are known to someone else.
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 Internet sites, never use a South Cambridgeshire District Council password or User ID to register a login.
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 Business and Operations Manager or Assistant Director (ICT), you should shut down your computer at the end of the working day. (NB. Always do this before switching it off).

Number	***Policy Item***
9.	Managers must ensure that access rights to systems are removed when staff leave Council employment, or such access rights are modified appropriately when staff move to a different job function. This should be instigated by contacting the Help Desk in advance of the change in status.
10.	Managers must ensure that the Help Desk is informed of any new starters in order for them to be registered on the appropriate systems and if necessary additional equipment ordered.
11.	Modems used by third parties to access systems 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 enabled by the ICT Team.

3. Information Policies

Number	***Policy Item***
1.	ICTwill 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.
3.	You must inform the Data Protection Officer of all new databases created that will be used to store personal data.
4.	If there is any doubt relating to the source or content of information, seek advice from the Help Desk before opening or saving the file.
5.	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.	Wherever possible, data should be stored on the shared folders on servers provided by ICT, such as the W, X, Y, and Z drives. This will ensure 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.

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 immediately.
2.	No employee should make or use unlicensed or illegal copies of copyrighted software under any circumstances.
3.	Never intentionally access or transmit computer viruses and similar software.
4.	All new software should be checked and installed by ICT, unless agreed otherwise with the ICT Business and Operations Manager.

Number	***Policy Item***
5.	Any software not installed and/or supported by ICT which: o Causes a technical problem o Is being used illegally o Is found to be offensive or inappropriate o Contravenes ICT Strategy requirements o 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.
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.

5. Computer Hardware/Physical Systems Policies

Number	***Policy Item***
1.	Always take reasonable steps to ensure the security of South Cambridgeshire District Council hardware when away from the premises. For example, never leave computers visible in your car.
2.	Personal computers should, where possible and appropriate, be sited away from windows and 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.	All equipment should be identified via a secure label ("asset tag") and included in the Council's inventory list maintained by ICT. Staff should report any deliveries of ICT equipment and other related hardware to ICT so that such marking can take place. Staff should report to the Help Desk any equipment which is not asset tagged.
5.	ICT must ensure that all ICT hardware complies with Health & Safety regulations. All staff are required to co-operate with ICT staff in their efforts to ensure Health & Safety regulations are being met.
6.	Under no circumstances should you connect non-South Cambridgeshire District Council hardware to the network.
7.	Do not install modems on South Cambridgeshire District Council PCs or laptops. If a modem is required, the request needs to be authorised by ICT Business and Operations Manager or Assistant Director (ICT).
8.	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.
9.	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 an ICT Computer Room managed by for this purpose. Where it is not practicable to locate equipment in the ICT Computer Room, please contact the Help Desk for advice on secure equipment location.
10.	Any potential security problems relating to computer hardware should be reported to the Help Desk..

Number	***Policy Item***
11.	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.

Section Three

Internet and Email Security & Usage Policy

1. Introduction

This section is intended for all staff and others offered access to Council ICT resources, such as elected Members, and relates to the specific use of Internet and email facilities. It includes:

Sub-section	***Subject Area***
Email Policies	Controls and guidelines relating to the use of email facilities provided by the Council.
Internet Use Policies	Controls and guidelines relating to the use of Internet access facilities provided by the Council.

The policies and guidelines have been agreed by the Council at Chief Officer level. Failure to comply with the policies and guidelines will be considered a serious offence and may lead to disciplinary procedures.

2. Email Policies

Number	***Policy Item***
1.	Incoming and outgoing email relating to the Council must be treated in the same way as formal business correspondence, and must follow normal authorisation and other procedures (such as correspondence logging and response monitoring). It should be noted that email can be used for documentary evidence in disciplinary proceedings, libel cases etc. even after it has been deleted.
2.	Official Council records communicated through email must be identified, managed, protected, and maintained as long as needed for ongoing operations, audits, data protection, legal actions, or any other known purpose.
3.	Emails received that invoke an emotional response and generate an impulse for an immediate response should only be responded to after due consideration and in a measured way.
4.	Where possible, highly confidential material should not be sent by email. Where this is not possible, encryption and/or password protection should be used. For further information please contact the Help Desk.
5.	All emails can be seen to originate from the Council. Therefore, the messages concerned shall not in any way contravene any legislation or this policy. In addition a corporate disclaimer will be added to all emails by default, using corporate content security software.
6.	Please note that deleting an email does not guarantee that the communication has been fully erased and therefore email must be treated as permanent.
7.	Council employees must not use an email account assigned to another individual to send or receive messages.
8.	If you receive a chain email or an email notifying you of a virus, do not forward it – contact the Help Desk first.
9.	Do not open attachments from anyone you do not know. Be very careful of external emails that you are sent from an unknown or unexpected source as attached files can often contain deliberate viruses.

Number	***Policy Item***
10.	You must not use email or the Internet send or receive email that is obscene or defamatory or intended to annoy, harass, intimidate or damage the reputation of another person or organisation, for example, by broadcasting unsolicited or libellous messages, by sending inappropriate mail, or by using someone else's name or User ID.
11.	Avoid responding to unsolicited mail. Responding to unsolicited mail only confirms that you have an active email address and could open you up to further solicitation that can clog your email inbox. If you are receiving repeated unsolicited mail from one source, please notify the Help Desk.
12.	If you are going to be away, a colleague should be entrusted to check your messages, or rules should be set on your computer system to automatically forward email to a colleague whilst you are away. On the other hand if you are sending a strictly confidential email, which should not be read by a delegated individual, then the message security should be set to 'confidential' and your email client configured to prevent access to such emails to anyone but the addressee. The Help Desk can help you to configure your email client.
13.	You should avoid sending excessively large emails or attachments. If you want to send a large file, typically a 5Mb or more attachment, then please contact the Help Desk for assistance.
14.	The Council's email system should be used primarily for the conduct of the Council's business. Responsible private use is allowed, but should take place in your own time.
15.	Never use the Council's email system for political lobbying or private business, or knowingly doing anything which is illegal under English law or the law of any other country.
16.	Users should be aware that email messages remain the property of the Council and can be accessed and monitored by authorised staff. Any private correspondence held on email systems will be treated in the same manner as business-related information and messages.
17.	Users should not represent their personal opinions as those of the Council.
18.	Users should refrain from using the Council's email system to send or receive high volumes of emails for bulk mailing, without the prior permission of your Director or Assistant Director (ICT).

3. Internet Use Policies

Number	***Policy Item***
1.	Access to Internet services must only be initiated by using Council-approved software and Internet gateways.
2.	Regular monitoring of Internet and email use will be undertaken by the Council, to ensure facilities are not being misused.
3.	A 'firewall' has been placed between the South Cambridgeshire District Council network and the Internet to protect our systems. Employees must not circumvent the firewall by using modems or 'network tunnelling' software to connect to the Internet.
4.	Content security software has been installed to monitor and control the viewing of Web content. This works on the principle of a list, automatically updated daily, of Web sites considered inappropriate for viewing. If you require access to a site which is reported as being blocked by the content security software, please inform your manager who can then request the Help Desk for the site, if appropriate, to be made accessible.
5.	Never use the Council's Internet account for political lobbying or private business, or knowingly doing anything which is illegal under English law or the law of any other country.
6.	Internet access facilities should be used primarily for the conduct of the Council's business. Responsible private use is allowed, but should take place in your own time. All users will be prevented from accessing specific types of site at any time by content security software. A list of these sites will be provided and maintained by a third party.

Number	***Policy Item***
7.	When providing your details to a Web site avoid giving out your Council email address since many Web sites will distribute your address to other parties, possibly resulting in unsolicited mail.
8.	Some organisations and companies accept orders for goods and services via the Internet. The fact that Internet access has been granted does not authorise you to place orders for yourself or in the name of the Council. Any orders placed in this way must be authorised through the normal procedures.
9.	You must not participate in any activities that could intentionally cause congestion and disruption of networks and systems.
10.	If you receive any offensive electronic information you must report it immediately to the Help Desk.
11.	It is unacceptable to use, display or transmit any information which is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or other objectionable material of any description including any material that may contravene any legislation.
12.	Never access or transmit information about, or software designed for, breaching security controls or creating computer viruses. Deliberate introduction of any damaging virus is a crime under the Computer Misuse Act 1990.
13.	You must not download software applications from the Internet. If in doubt, contact the Help Desk. For clarity, software applications include games & screensavers as well as demonstration, evaluation free and shareware software.
14.	Do not take part in 'chat lines', newsgroups or online games, as Internet Relay Chat (IRC) and similar functions are susceptible to virus transmission. If your work requires the legitimate use of 'chat lines' or similar messaging facilities please contact the Help Desk for advice and guidance.
15.	You must not transgress copyright law in any way including downloading copyright material, or making South Cambridgeshire District Council copyright material accessible to others.
16.	Web sites you visit may implant software known as 'cookies' on your machine. Some of these cookies serve a useful purpose, for example to facilitate e-commerce transactions, but some are used to track your movements on the Internet. Check your 'Cookie' files and consider deleting those you do not want. For more information contact the Help Desk.
17.	Inappropriate use of the Internet will be considered a disciplinary offence and may lead to dismissal. It could also lead to criminal or civil action if illegal material is involved or if legislation, such as the Data Protection Act, is contravened.
18.	Above all use common sense. Be smart when you are on the Internet, and maintain a healthy dose of scepticism. Use caution when revealing personal information, such as your physical address.

Section Four

ICT Security Policy Management

1. Introduction

This section provides part of the framework for security and control over the use of ICT by introducing a set of reference guidelines for managers and staff to establish and maintain a controlled environment for Internet and Email Security. This section is intended for use by management staff to help them manage the policies and understand why the Council's security controls are needed.

In summary, South Cambridgeshire District Council must provide sufficient control safeguards and security organisation to underpin the Council's ICT Security Policy and Usage Guidelines. Without these, the long-term health of the Council is at risk.

Definition of Security

ICT Security can be defined as "*the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (including hardware, software, firmware, information/data, and telecommunications)*".

The risk concerns the following categories of loss:

Category	***Description***
Confidentiality of information	Confidentiality refers to the privacy of personal or corporate information. This includes issues of copyright.
Integrity of data	Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disk fails, or subtle, such as when a character in a file is altered.
Assets	The assets that must be protected include: o Computer and peripheral equipment o Communications equipment o Network infrastructure including WiFi connectivity o Computing and communications premises o Power, water, environmental control, and communications utilities o Supplies and data storage media o System computer programs and documentation o Application computer programs and documentation o Information
Efficient and appropriate use	Efficient and appropriate use ensures that Council ICT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

System availability	Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components.

The potential causes of these losses are termed ‘threats’. These threats may be human or non-human, natural, accidental, or deliberate. Examples of threats, particularly relating to email, are provided in this section.

Reasons for ICT Security

Confidentiality of information is mandated by common law, formal statute, explicit agreement, or convention. Different classes of information warrant different degrees of confidentiality.

The hardware and software components that constitute the Council’s ICT assets represent a sizeable financial investment that must be protected. The same is true for the information stored in its ICT systems, some of which may have taken huge resources to generate, and some of which can never be reproduced.

The use of Council ICT assets in other than a manner and the purpose for which they were intended represents a misuse of valuable Council resources, and possibly a danger to its reputation or a violation of the law.

Finally, proper functionality of ICT systems is required for the efficient operation of the Council. A number of systems are of paramount importance to enable the Council to discharge its responsibilities and carry out its business.

2. Responsibilities

To build and maintain an appropriate security environment requires the organisation and management of data security within South Cambridgeshire District Council.

The following responsibilities have been identified and assigned.

Policy Management

Overall Policy Approval

Approval of the ICT Security Policy and Usage Guidelines is vested with the Management Team of the Council.

Management of the ICT Security Policy and Usage Guidelines

Information security is a business responsibility that must be supported by Management. A process must be in place to ensure that information security requirements are monitored at a high level. The Assistant Director (ICT), will act as the security adviser, to:

- Monitor exposure to threats to information assets.
- Review and monitor any security incidents.
- Originate, approve and support initiatives to improve security.
- Promote awareness of information security throughout the Council.
- Consider security measures for new systems or services.

Formulation, review and maintenance of the ICT Security Policy and Usage Guidelines is the responsibility of the Assistant Director (ICT) and the ICT Business and Operations Manager.

Policy Implementation.

Each staff member of the Council will be responsible for implementing the policy.

Assistant Director (ICT)

It is the responsibility of the Assistant Director (ICT) to:

- Provide specialist advice on computer security
- Where required, provide a security ‘sign-off’ for all new computer systems and major system enhancements during development and before implementation
- Evaluate all new computer security products proposed for implementation in South Cambridgeshire District Council systems
- Determine a strategy for computer security training for all staff and ensuring its implementation
- Authorise removal of any ICT assets from Council property, as advised by System Owners (see section 2.5) and ICT staff.
- Investigate any suspected security breaches with the Internal Auditor
- Maintain security documentation

SUMIT (Service Users Meeting with IT) Group

It is the responsibility of this group, at their meetings, to:

- Review any identified security risks
- Make appropriate recommendations for the updating of the ICT Security Policy and Usage Guidelines.

System Owners

It is the responsibility of System Owners (those with overall responsibility for a system and its information), in conjunction with their IT Liaison Officers, to:

- Produce and maintain user system access rights
- Ensure that user's access rights are removed from the system when their jobs change or they leave the Council
- Notify the Helpdesk of users to be deleted from their systems, so that network access rights to the system can be removed
- Authorise requests for extended/out of hours network access for staff
- Ensure all systems are registered under the Data Protection Act
- Determine appropriate access levels
- Ensure all computer assets are accounted for and have a nominated 'owner' who will take appropriate steps to secure that asset
- Authorise removal of ICT assets from Council property in-conjunction with the Assistant Director (ICT).
- Ensure all incidents, breaches or potential incidents of computer security are reported via the Assistant Director (ICT) as soon as possible
- Ensure all staff adhere to the Copyright, Misuse and Data Protection Acts and the organisation's ICT Security Policy and Usage Guidelines

System Users

It is the responsibility of system users (any person making use of the system in the course of their normal duties) to:

- Ensure the security of hardware and software assets placed in their care
- Protect ICT equipment against theft and malicious or accidental damage
- Comply with the ICT Security Policy and Usage Guidelines.

Data Protection Officer

- Produce and maintain Data Protection Act Registrations
- Produce and maintain Risk Register associated with the Act

ICT Business and Operations Manager

It is the responsibility of the ICT Business and Operations Manager to:

- Produce, maintain and test the ICT Disaster Recovery Plan
- Produce and maintain an ICT equipment Asset Register and Security mark all hardware
- Maintain access controls for all systems
- Ensure the security of hardware and software assets

- Ensure Information Security is given adequate consideration in procurement
- Ensure compliance with effective use of software licences including periodic software audits
- Protect ICT equipment against theft and malicious or accidental damage
- Administer User ID's and the associated system access rights in conjunction with System Owners
- Take daily backup copies of data held on file servers, keep them safely and for a period agreed as part of the ICT Backup strategy
- Comply with security policy
- Ensure that virus protection is monitored and continually upgraded
- Provide advice about these security guidelines

Availability

It is intended that this ICT Security Policy and Usage Guidelines be accessible in its entirety via the Council's Intranet (In-Site). There is the requirement that all users of Council ICT resources be familiar with relevant sections of this policy; the policy should be covered as part of the induction of new staff.

Changes

The ICT Security Policy and Usage Guidelines is to be a 'living' document that will be altered as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers, etc.

Major changes will be made in consultation with the Management Team, and with the approval of the Chief Executive.

The Assistant Director (ICT) will approve minor changes.

3. ICT Infrastructure Controls

In order to facilitate the policies defined in the ICT Security Policy and Usage Guidelines the Council has:

- Installed a SonicWALL firewall solution to prevent unauthorised access to the network.

- Installed the Barracuda 'Email Filter', which intelligently scans email messages for offensive words and phrases in order to prevent them entering the email system, automatically attaches legal disclaimers to email, scans attachments and other security functions.

- Installed the SonicWALL 'Web Filter' Internet content security solution, which allows the Council to monitor and control Web transfers, including Hypertext transfer protocol (HTTP), secure Hypertext transfer protocol (HTTPS) and file transfer protocol (FTP).

- Installed the SonicWALL SSL-VPN 2000 appliance for secure access to the network and associated services.

- Implemented the SOPHOS anti-virus solution for all PC's, Servers and Laptops.

- Implemented a Windows 2003 Active Directory infrastructure for the management of network users, internal server and workstation security.

- Implemented Quest 'AfterMail' to provide a email archive solution and compliance with the requirements of the Freedom of Information Act.

- Implemented LANDesk 8.0 and Visual Audit X3 to provide accurate inventory management of physical hardware assets and software licenses.

The use of these tools will assist in the monitoring and control of Internet, email and other ICT security, though it should be recognised that such facilities, whilst valuable tools, require 'common sense' personnel and information management in order to be most effective.

4. Guidance Notes on ICT Security

Electronic mail or email is one of the most popular uses of the Internet. With access to Internet email, one can potentially correspond with millions of people worldwide.

It is however, easy to have email 'accidents'. An email message can be sent instantly with little hope of retrieval. A single keystroke or mouse-click can misroute the message. Email messages may be archived for years, so that an ill-considered remark can return to haunt the sender later. Email folders can grow until the email system becomes unstable. Wrongly configured discussion group software can send messages to the wrong groups. Errors in email lists can flood the subscribers with hundreds of error messages. Sometimes error messages will bounce back and forth between email servers, multiplying until they crash the servers.

When an organisation's internal email system is connected to the Internet, the effect of accidents can be multiplied a thousand fold.

Email Monitoring Guidelines

Email Protocol and Guidelines

The relevant policies and guidelines should be made clear and easily available to Council staff. This can be achieved by publishing the document on the Council's Intranet.

Contract of Employment

All Council staff should receive training in the use of email and to be made aware of the kinds of monitoring proposed. This will enable the Council to escape liability for the acts of employees to a certain extent. An appropriate sign-off should be attached to the ICT Security Policy and Usage Guidelines to indicate that the employee has read, fully understands and adheres to the policy.

Vetting Emails

If the Council intends to vet their employees' email then this should be clearly stated in the contract of employment otherwise the employee might be able to claim that their right to privacy has been breached. This is as a result of the Human Rights Act that is likely to impose restrictions on what an organisation can do. Moreover the Council should take care not to fall foul of the Data Protection Act. The Council should state that an employee's use of the email is not private and is subject to Council scrutiny. This will help also to discourage misuse.

Confidentiality Notice

A disclaimer containing a confidentiality notice should be considered within a standard Council email format and is similar to those often found on faxes. The clause is designed to preserve the confidentiality of the Council's information in the event that any unauthorised access to it occurs. It will not exclude liability on defamation but can limit liability on negligence.

Personal Emails

The ICT Security Policy and Usage Guidelines define limits on personal use of email; in the same manner as personal use limits are defined for telephones and fax machines.

Sending email from the Council's address can be likened to sending a letter on Council letterhead. If you use your Council account to send email to an email discussion group, it may appear as though the Council endorses whatever opinions have been put in the message.

The key is to educate Council staff to the legal implications. It must be made clear that their messages are in no way associated with the Council and that the guidelines in the ICT Security Policy and Usage Guidelines are followed.

Deleting Emails

It should be brought to the attention of the Council employees that deleting an email from the desktop client (Outlook 2000 or Outlook 2003) does not remove all copies of the email. It remains on the system and additional copies of the email may have been forwarded to another party or saved to a backup disk To comply with the requirements of the Freedom of Information Act, the Council uses the email archiving system (AfterMail) to create a permanent archive of all email messages sent to, from or via the Councils email system.

What needs to be emphasised is that in a dispute it is possible for the Courts to order the Council to preserve their email as evidence. This can be highlighted in the recent Norwich Union case, where hard copies of email were used as evidence. This case highlights the dangers where employees have access to the Internet or in-house email systems, and is seen as the biggest action in the UK arising out of defamation by email – resulting in the payment of £450,000 in damages and costs.

Statements of Facts Untrue

Statements of facts that damage the reputation of the person or organisation or holds him/her up to hatred, ridicule or contempt are libellous. It is important to note that emails need not be insulting to damage reputation. Therefore, if expressing an opinion it is important to ensure that the relevant facts are set out. Council employees should take great care in what they say so that they do not bind the Council to a contract it does not want or in terms it does not agree, and that they do not write anything that would jeopardise the integrity or reputation of the Council. An aggrieved party can sue in the jurisdiction from where the libel is published.

Insurance Cover

Consideration should be given to extending insurance cover to include liability in defamation, if this is not already included in existing insurance provision.

Highly Confidential/Sensitive Information

Employees should be advised that where possible highly confidential material should not be sent by normal email. Where confidential material must be sent via email, an encryption technique should be employed to comply with Council policy. This should also be part of the training given to employees especially Members, senior managers and directors of the Council.

Delegating Email

The public increasingly expects a rapid response from email; therefore if a Council employee is going to be away, a colleague should be entrusted to check messages. This can be done by setting rules in the email client to forward email to a delegate. On the other hand if a message is strictly confidential and must not be seen by anyone except the recipient then the message security should be set to ‘confidential’ which means the delegated colleague is unable to read the message.

Email Threats

The most common mail transfer protocols (SMTP, POP3, IMAP4) do not typically include provisions for reliable authentication as part of the core protocol, allowing email messages to be easily forged. Nor do these protocols require the use of encryption that could ensure the privacy of email messages. These ‘weaknesses’ of email introduce the following threats:

Impersonation

The sender address on Internet email cannot be trusted, since the sender can create a false return address, or the header could have been modified in transit, or the sender could have connected directly to the SMTP port on the target machine to enter the email.

Eavesdropping

Email headers and contents are transmitted ‘in the clear’. As a result, the contents of a message can be read or altered in transit. The header can be modified to hide or change the sender, or to redirect the message.

Mailbombing

Mailbombing is an email-based attack. The attacked system is flooded with email until it fails. For example Motorola was flooded by emails when an unidentified individual sent out an email claiming that the company were offering free WAP phones to the first 10,000 replies to an email account based at Motorola. This flooded Motorola’s messaging system in the UK and was seen as an extremely malicious attack on the organisation.

Junk and Harassing Mail

Since anyone in the world can send you email, it can be difficult to stop someone from sending it to you. If you give your Council email address to any Web site, they can potentially pass that address onto a number of different sources.

ICT Housekeeping Guidelines

The following guidelines may assist in managing ICT security risks:

Documentation

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalising operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

Maintenance

System maintenance requires either physical or logical access to the system. Support and operations staff, hardware or software vendors, or third-party service providers may maintain a system. Maintenance may be performed on site, or it may be necessary to move equipment to a repair site. Maintenance may also be performed remotely via communications connections. If someone who does not normally have access to the system performs maintenance, a security vulnerability is introduced.

Supervision of maintenance personnel may prevent some problems, such as ‘snooping around’ the physical area. However, once someone has access to the system, it is very difficult for supervision to prevent damage done through the maintenance process.

Many computer systems provide maintenance accounts. These special login accounts are normally preconfigured at the factory with pre-set, widely known passwords. It is critical to change these passwords or otherwise disable the accounts until they are needed.

One of the most common methods hackers use to break into systems is through maintenance accounts that still have factory-set or easily guessed passwords.

Procedures should be developed to ensure that only authorised maintenance personnel can use these accounts. If the account is to be used remotely, authentication of the maintenance provider can be performed using a variety of methods including secure SSL-VPN. This helps ensure that remote diagnostic activities actually originate from a known user at the vendor's site. Other techniques can also help, including encryption and decryption of diagnostic communications, strong identification and authentication techniques, such as tokens (e.g. the RSAsecureID standard supported by Windows 2003), and remote disconnect verification. Wherever possible, all such remote connections to the SCDC network should be facilitated by a secure SSL-VPN link.

Anti-Virus Regulations

To protect Council computer systems against viruses and virus detection, prevention measures in conjunction with appropriate user awareness procedures should be implemented. Anti-Virus procedures should include:

- processes and appropriate staff awareness procedures should be in place to prevent the introduction of viruses into the Council
- ICT Section must ensure that Virus scanning software is kept up-to-date, and is installed on all systems
- ICT Section have responsibility for carrying out virus scanning on all software and data originating externally
- all PCs must be scanned automatically using up-to-date SOPHOS anti-virus scanning software
- any diskette of uncertain or unauthorised origin must be checked for viruses using virus scanning software before use
- all virus occurrences should be reported to the Help Desk, logged and treated as security incidents
- all staff should be aware of the procedures for dealing with virus incidents

Copyright

To ensure unauthorised software is not used:

- Software licences shall always be complied with and the use of unauthorised software prohibited
- Copying of software, other than by ICT for back-up purposes, is forbidden and may lead to disciplinary procedures being invoked
- ICT will undertake regular audits to ensure compliance with terms of licences
- Procedures should be developed for reporting the discovery of unauthorised software to the Assistant Director (ICT)
- Any unauthorised software may be isolated, disabled or removed by ICT staff
- All contracts with external service providers will insist that necessary licences are held by ICT for any products used as part of the service

Section Five

Internet and Email Filtering Policy

1. Introduction

This section is intended to cover the software solution used to monitor Internet and email use within the Council.

South Cambridgeshire District Council must provide sufficient control safeguards and security organisation to underpin the Council's ICT Security Policy and Usage Guidelines. The goal of this section is to outline the Internet access controls and email filtering to be implemented to protect the Council's ICT resources.

The Council's resources, including the network, servers, computers, email & voicemail, are provided for business purposes. At any time and without prior notice the Council maintains the right & ability to examine any systems and inspect and review any and all data recorded in those systems. Any information stored on a server or computer, whether information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by the Council. This scrutiny helps ensure compliance with Council policies and the law.

In order to ensure compliance with its ICT Security Policy the Council will employ monitoring software to check on the use and content of email. The Council specifically reserves the right for authorised personnel to access, retrieve, read and delete any communication that is created on, received through or sent in the email system, to ensure compliance with Council policy and any relevant legislation.. Such monitoring will be used for legitimate purposes only and operate under the monitoring code of conduct outlined in the ICT Security Policy.

The objectives of the ICT Security Policy and Usage Guidelines are:

- To encourage effective and positive use of the Council's resources
- To avoid security threats by promoting awareness & good practice
- To shield the Council against potential liability

Common Areas of Risk

Several common areas where there is a risk to the Council's ICT systems or potential for abuse of systems are identified below.

Employee Productivity

The information and resources available through the Internet can help employees to be more productive and effective. The Council's use of the Internet will increase as the implementation of electronic government become a reality. Most employee use of the Internet and email systems will be legitimate, but with access to services such as sports scores, games or chat rooms there is a risk that some employees could abuse their Internet access. The Council is obliged to take reasonable steps to monitor use of its Internet connection.

Network Performance

The Council has a leased line connection to the Internet but the combination of recreational surfing and bandwidth-intensive activities such as streaming audio and video, MP3 downloads and image downloads can have a significant impact on network performance that impedes 'business' traffic.

Security

The Council's permanent connection to Internet opens the Council's ICT network and systems to potential security breaches. Network security issues become more acute when the Council's network is connected to the Internet and the Council needs to take reasonable steps to maintain the security of its data and networks and to ensure that its systems are not compromised by the introduction of viruses, malicious code or 'Trojan horses', either by email or by download from web sites.

Legal Liability

The Council aims to reduce its liability by identifying areas of risk and mitigating for these. Areas of risk that are commonly identified are:

- Letting employees surf anywhere on the Internet
- Sexual harassment as a result of bringing objectionable or sexually explicit material into the workplace.
- Copyright infringement through the use of material retrieved such as software programs or photographs which have been used 'because it's on the web'
- Misrepresentation can also occur unintentionally, particularly through the use of email. Unless providing specific advice or guidance as part of their job function, employees should know and make it clear to the people with whom they communicate that opinions expressed via email and other electronic media are their own, not the Council's.

Adverse Publicity

Several major international companies have been forced to dismiss employees that were found guilty of accessing illegal and offensive material through the Internet and for circulating messages that were not intended for them. Adverse publicity could be very damaging for the Council and its staff.

2. Web and Email Filtering Software

The Council has purchased a subscription to web and email filtering systems. These systems provide the facility to implement and monitor the Council's security policy.

Web Filtering

Blocking Sites

It is impossible to expect employees to know about the content of every site that they visit, sites that they are referred on to from other sites or search results pages. To prevent staff accidentally visiting sites that are inappropriate or liable to cause offence or distress to themselves or their colleagues the Council has chosen to subscribe to a maintained list of categorised sites that can be used to block access.

The current category list is attached as Appendix 1, showing which categories will be allowed or blocked. Management Team, advised by the Assistant Director (ICT), has agreed this list. Updates and changes to this list will be made as categories change, in agreement with Management Team.

When users try to access a blocked site they will be presented with an error page, stating the site's category and steps they can take to access the site if they have a legitimate need to do so. Attempted access to blocked sites will be recorded and will form part of a monthly report that will be used to monitor the effectiveness of the policies or to modify whether the categories in Appendix 1 are allowed or blocked.

Monitoring of Sites and Traffic

The web filtering system enables monitoring and logging of web traffic, including statistics such as sites visited and traffic passed. All information will be logged to a database to allow a set of standard management reports to be run on the logs. The Assistant Director (ICT) and/or the ICT Business and Operations Manager will review monthly reports to show which sites have been visited, how many times these sites have been visited and how much data has been transferred. These reports will be primarily of the 'Top Ten' variety and will be used to identify sites that would benefit from being cached on the Council's web system, thus reducing usage of Internet network bandwidth.

The objectives of analysing these reports are:

- To monitor exposure to threats to information assets.
- To review and monitor any security incidents.
- To originate, approve and support initiatives to improve security.
- To ensure compliance with the ICT Security Policy and Usage Guidelines.

Inappropriate Activity

In cases of persistent inappropriate activity ICT will be requested to inform the Assistant Director (ICT). The matter may then be dealt with in association with the user, the user's line manager and the HR section, in line with current disciplinary procedures.

Email Management.

Electronic mail or email is one of the most popular uses of the Internet. With access to Internet email, one can potentially correspond with millions of people worldwide.

It is however, easy to have email 'accidents'. An email message can be sent instantly with little hope of retrieval. A single keystroke or mouse-click can misroute the message. With the Council's internal email system connected to the Internet, the effect of accidents can be multiplied considerably. Email messages may be archived for years, so that an ill-considered remark can return to haunt the sender later

The addition of email filtering software will allow incoming email to be scanned and, if necessary cleaned or quarantined before it is allowed onto the Council's network. Similarly outbound email can be checked to prevent Council employees inadvertently passing inappropriate or infected email messages on to external organisations.

Whenever the email filtering software is used to block, delay or quarantine messages the sender and/or recipient will automatically be notified, so that, if necessary, appropriate action can be taken to allow the message through.

Inbound email

All inbound email will be checked for viruses, worms, trojans, malware and inappropriate content.

Outbound email

All outbound email will be checked for viruses, worms, trojans, malware and inappropriate content.

.

Email attachments

Attachments of certain types will be restricted. The objectives of restricting certain attachments are:

- To prevent the introduction of viruses that are transmitted as a particular type of attachment, such as Visual Basic Script (.vbs) mailing worms where the Council does not use such attachments.
- To prevent use of network bandwidth by inappropriate file attachments.
- To prevent large attachments interfering with other network usage.

Attachments may be deleted, quarantined or rescheduled for sending outside of normal business hours, depending on the type of attachment and the perceived risk to the Council.

Email Circulars, Mass Mailings and Chain Emails

The email filtering system has the ability to detect email circulars, mass mailings and chain emails. These types of emails are identified from a list of known messages maintained by Barracuda. The email filter system will be used to filter these messages before they reach employees' mailboxes, avoiding the distress that these messages often cause and preventing the messages from being propagated further. In addition the email filtering system will be used to prevent bulk mailings to external recipients, as these are often a symptom of email mass-mailing worm viruses. The sender will automatically be notified if they have had bulk-mailed messages blocked, so that these messages can be allowed if they are legitimate.

Legal Disclaimer & Confidentiality Notice

The email filtering system allows a disclaimer containing a confidentiality notice to be attached to all outbound email messages. This disclaimer will be developed, in association with the Council's Legal Section, and will be implemented under the supervision of Management Team. Any future changes to this disclaimer will be proposed by the Assistant Director (ICT) to Management Team and be implemented with their ratification.

Email Message Content

The email filtering system has the ability to check for obscenities and profanities. A list of common obscenities and profanities is supplied and maintained by the system vendor and weighting is applied to each word. Scores are totalled for a message and the message can be blocked once a threshold has been reached. This message can be used to prevent staff from receiving offensive or abusive messages and can be applied to both internal messages (on the Council's Microsoft Exchange Server) and external email (messages to or from Internet addresses).

Section Six

Web and Email Filtering Code of Conduct

1. Introduction

This section is intended to provide guidance for the system administrators of the web and email filtering system used to monitor use by Council staff. It is included within the ICT Security Policy and Usage Guidelines to provide transparency of operation to all staff; those employed by the Council and those contracted to provide services to the Council.

2. Code of Conduct

It is expected that all users will deal with email and web access in a professional manner. To ensure that the requirements are clear they are detailed below.

To build and maintain an appropriate security environment requires the organisation and management of data security within South Cambridgeshire District Council.

Monitoring and Reporting

Automatic Monitoring

All monitoring of Internet and email use will be carried out by automated systems configured to a standard agreed by Management Team.

No monitoring of specific messages or specific users will be carried out, except where authorised by a Chief Officer (usually as part of a Council disciplinary or grievance process).

In the event that a system administrator accidentally or unintentionally opens any email messages the content of such messages will be treated as confidential and must not be disclosed or discussed.

Email messages should be treated in the same manner as physical post. Inappropriate or unauthorised opening of messages will be dealt with in the same manner as unauthorised opening or tampering with physical post.

Reporting

Standard reports will be used wherever possible to provide management information to the Assistant Director (ICT) and/or the ICT Business and Operations Manager. These reports may also be presented, Management Team, SUMIT, department or section heads, or other groups/committees.

These reports will only be used to:

- Monitor exposure to threats to information assets.
- Review and monitor any security incidents.
- Originate, approve and support initiatives to improve security.
- Promote awareness of information security throughout the Council.
- Consider security measures for new systems or services.
- Ensure compliance with the ICT Security Policy and Usage Guidelines

Persistent Inappropriate Use or Abuse of Email System

Persistent abuse of Internet access or the email system should be considered a security incident and should be reported to the assistant Director (ICT) and/or ICT Business and Operations Manager as a security incident using the usual reporting methods.

Responsibilities

Assistant Director (ICT)

It is the responsibility of the Assistant Director (ICT):

- To review Internet usage on a regular basis
- To review number of blocked sites that users have attempted to access
- To review the number of security incidents
- To make recommendations regarding changes in the ICT Security Policy and Usage Guidelines to the ICT Steering Group
- To make recommendations regarding changes in the configuration of the web and email filtering systems to the ICT Steering Group
- To ensure that staff are made aware of the filtering and monitoring which is taking place

Management Team

It is the responsibility of Management Team:

- To debate & agree proposed changes to the web and email filtering systems
- To review reports detailing activity or levels of use which raise cause for concern.

ICT Business and Operations Manager

- To produce regular and ad hoc usage reports
- To implement configuration changes to the email filter and web filter systems
- To administer and maintain email filter and web filter systems
- To ensure that only authorised users have access to the Internet
- To ensure that the email server, web filter and email filter systems are kept secure
- To take reasonable action to ensure the security of the Council's ICT network

Changes

Changes to the configuration of the web and email filtering systems will be subject to normal change control procedures. All major changes will be logged and tracked, providing an audit trail which will include details of who requested the work and when it was completed/implemented.

Any changes that are made by to the web filter and email filter systems, as an emergency measure to ensure the security of the Council's network, will be notified to the Assistant Director (ICT) or ICT Business and Operations Manager.

Issues

All Council staff should be made aware of the kinds of monitoring proposed. An appropriate sign-off should be attached to the ICT Security Policy and Usage Guidelines to indicate that the employee has read, fully understands and adheres to the policy, before access to ICT systems is given. The fact that web access and email will be monitored should be made clear to all employees.

In the case that any member of staff has an issue relating to the way that their email or Internet access has been monitored it should be discussed with their line manager in the first instance. If the issue cannot be resolved with the line manager the issue should be escalated to the Assistant Director (ICT).

Appendix 1 - Web Filter Category Settings

The following Web Filter category settings will apply..

Where sites are blocked these may be allowed to specific users, if justified by business requirements.

Category	Status	
Adult/Sexually Explicit	Block	
Advertisements	Block	
Arts & Entertainment		Allow
Chat	Block	
Computing & Internet		Allow
Criminal Skills	Block	
Drugs, Alcohol & Tobacco	Block	
Education		Allow
Finance & Investment		Allow
Food & Drink		Allow
Gambling	Block	
Games	Block	
Glamour & Intimate Apparel	Block	
Government & Politics		Allow
Hacking	Block	
Hate Speech	Block	
Health & Medicine		Allow
Hobbies & Recreation		Allow
Hosting Sites		Allow
Job Search & Career Development		Allow
Kid's Sites		Allow
Lifestyle & Culture		Allow
Motor Vehicles		Allow
News		Allow
Personals and Dating	Block	
Photo Searches		Allow

Category	Status	
Real Estate		Allow
Reference		Allow
Religion		Allow
Remote Proxies	Block	
Sex Education	Block	
Search Engines		Allow
Shopping		Allow
Sports		Allow
Streaming Media	Block	
Travel		Allow
Usenet News	Block	
Violence	Block	
Weapons	Block	
Web-based Email		Allow

Appendix 2 – Email Filter Settings

Basic System Configuration

- Disable SMTP relay, except for allowed hosts (Exchange Server) to prevent mail relay through the Council network
- Scan inbound and outbound email for viruses. If the email message is infected quarantine the message and notify the sender and recipient.
- Add legal disclaimer to all outbound email. The following disclaimer will be applied:

"Privileged/Confidential Information may be contained in this message. If you should not have received it, tell me and delete it without forwarding, copying or disclosing it to anyone. The Council does not represent or warrant that it or any attached files are free from computer viruses or other defects. It and any attached files are provided, and may be used, only on the basis that the user assumes all responsibility for any loss, damage or consequence resulting directly or indirectly from them or their use. Any views or opinions presented are those of the author and do not necessarily represent those of South Cambridgeshire District Council unless stated otherwise.

All e-mail sent to or from this address will be processed by South Cambridgeshire District Corporate E-mail system/ Email Archiving system and may be subject to scrutiny by someone other than the addressee.

This email will also be kept for a period of time before it is destroyed.

The South Cambridgeshire website can be found at http://www.scambs.gov.uk"

File attachments

Email file attachments will be dealt with in the following manner:

File	Type	Route	Action	Notification
.vbs	Visual Basic Script	In & out	Quarantine	Sender & recipient
.exe	Executable file	In & out	Quarantine	Sender & recipient
.zip	WinZip compressed file	In	Quarantine	Recipient
		Out	Quarantine	Sender
.jpg	JPEG picture	In & out	Allow	

File	Type	Route	Action	Notification
.avi	Video file	In	Quarantine	Recipient
.avi	Video file	Out	Quarantine	Sender
.mpg	MPEG video file	In	Quarantine	Recipient
.mpg	MPEG video file	Out	Quarantine	Sender
.mp3	Music files	In & Out	Block	Sender
	Large attachments more than >1 Mb addressed to Sheltered Housing schemes or Members	Out	Block	Sender
	Large attachments more than> 5 Mb	Out	Reschedule to send out overnight	Sender

Risk Filter

Risk Filter is a list of known mail messages, subject lines and/or senders maintained and updated by Barracuda. Risk Filter will be used to automatically block the following types of messages:

- Spam
- Chain letters
- Junk Mail
- Bulk mailing

Lexical Analysis

Lexical analysis of email messages allows for better control of inappropriate use..

Lexical analysis allows threshold values to be set for a list of terms and phrases maintained by Barracuda. Messages could be quarantined or deleted, based on threshold values. Further actions or alerts could be instigated if/when certain of these rules are triggered.

This policy is applied to internal (Outlook/Exchange Server) and external (inbound & outbound Internet) email messages.

Appendix 3 – Internet Acceptable Use Policy

The Council abides by an Internet Acceptable Use Policy as part of its contract for Internet services. A copy of the policy is included below.

ACCEPTABLE USE POLICY

This Acceptable Use Policy specifies the actions prohibited to users of the SCDC / CCN Internet Network. Users may be defined as "anyone who uses or accesses the SCDC / CCN Network or Internet service". The Council reserves the right to modify this Policy at any time. Any modifications to this Policy will be made when the Council feels it is appropriate and it is the User's responsibility to ensure their awareness of any such changes.

ILLEGAL USE

The SCDC / CCN Network may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or intellectual property right used without proper authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

THE NETWORK

.

The SCDC / CCN Network may be used to link into other networks worldwide and the user agrees to conform to the acceptable use policies of these networks.

In addition the user undertakes to conform to the Internet protocols and standards.

The user may not circumvent user authentication or security of any host, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, or network (referred to as "denial of service attacks").

Without prejudice to the foregoing, the Council considers that any application that overloads the SCDC / CCN by whatever means will be considered as making profligate use of the SCDC / CCN Network and is as such NOT allowed. Use of IP multicast other than by means provided and co-ordinated by the Council is likewise prohibited.

Users who violate systems or network security may incur criminal or civil liability. The Council will fully co-operate with investigations of suspected criminal violations, violation of systems or network security under the leadership of law enforcement or relevant authorities.

SYSTEM AND NETWORK SECURITY

Violations of system or network security are prohibited, and may result in criminal and civil liability. The Council will investigate incidents involving such violations and will involve and will co-operate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorisation of the owner of the system or network;

Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network;

Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.

If approached with complaints relating to any of the above violations, The Council will co-operate with investigations in order to bring such misuse and violations to an end.

E-MAIL

It is explicitly prohibited to send unsolicited bulk mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements) etc.

It is also explicitly prohibited to allow others to send unsolicited bulk mail messages either directly or by relaying through the Councils systems. For the avoidance of doubt, Users may not forward or propagate chain letters nor malicious e-mail.

A User may not solicit mail for any other address other than that of the user, except with full consent of the owner of the referred address.

USENET NEWS

All Users of the SCDC / CCN Network are advised that access to UseNet News Groups is restricted and only allowed where specific business need has been identified.

Where Users are given access to the UseNet service, they should, before using the service, familiarise themselves with the contents of the following newsgroups : news.newusers.questions; news.announce.newusers; and news.answers

Excessive cross posting (i.e., posting the same article to large numbers of newsgroups) is forbidden.

Posting of irrelevant material to newsgroups (also known as USENET spam) is also forbidden.

Posting binaries to a non-binary newsgroup is forbidden.

INTERNET WATCH FOUNDATION

The Council shall abide by advice given by the independent industry body The Internet Watch Foundation ("IWF") in relation to content of the Internet. For further information regarding IWF and its policy, please refer to www.internetwatch.org.uk

Complaints regarding Illegal Use or System or Network Security issues, Email abuse, USENET abuse or Spamming should be sent to the Assistant Director (ICT)