



ICT Acceptable Use Policy

Document Management

Document Disclaimer

This document is issued only for the purpose for which it is supplied.

Document Owner

This document is produced and owned by Staffordshire County Council (SCC). It is the responsibility of the Information Security Team to review and update the document annually and whenever necessary.

Document Control

This document is controlled and maintained according to the documentation standards and procedures of Staffordshire County Council. All requests for changes to this document should be sent to the author(s).

Any new issues of this document will be located on the corporate intranet and will be sent to the recipients as defined within the distribution list maintained by the author(s).

Distribution List

Copy	Name
1	SICT Senior Management Team and Directorate ICT Managers

Change History

Version	Author(s)	Reason for Change	Date
0.1	David Sharkey and Manjot Dhani	Initial draft version for distribution and review comments	04/05/2005
0.2	DJS, MSD	Second draft incorporating comments	25/08/2005
0.3	Pat Yates	Incorporating Mailbox and Internet usage limits	01/03/2006
0.4	Pat Yates	Security Forum amendments	03/08/2006
0.5	DJS, MSD	Security Awareness Training amendments	27/11/2006

Change Approval

The ICT Acceptable Use Policy is reviewed regularly and amended as necessary. The Information Security Forum will agree significant changes to the policy.

CONTENTS

1. INTRODUCTION	5
2. PURPOSE	5
3. SCOPE	5
4. REPORTING SECURITY INCIDENTS	5
5. GENERAL USE AND OWNERSHIP	6
5.1 Hardware	6
5.2 Software.....	7
5.3 Computer Viruses.....	7
5.4 Transfer or Storage of Data.....	8
6. INTERNET AND EMAIL USE	9
6.1 Access to Email and Internet Services	9
6.2 Prohibited use.....	10
6.3 Copyright.....	11
6.3.1 Copyright Documents	11
6.3.2 Copyright Emails	11
6.3.3 Copyright Software	11
6.4 Publishing information	11
6.4.1 Information on the Internet.....	11
6.4.2 Transmitting Information	12
6.5 Confidential or sensitive information	12
6.5.1 Data Protection Act	12
6.5.2 Sending Confidential or Sensitive Information via Email	12
6.5.3 Email Disclaimer	12
6.6 Bulletin board	13
6.7 Monitoring and Recording	13
6.7.1 Network Monitoring	13
6.7.2 Email Monitoring	13
6.7.3 Internet Usage Monitoring.....	13
7. IF YOU BREAK THIS POLICY	14

8. FURTHER GUIDANCE OR TRAINING.....	14
9. GLOSSARY	15
10. POINTS OF CONTACT.....	15
11. RELATED DOCUMENT LOCATIONS.....	15
12. APPENDICES	16
12.1 Appendix 1 - Email code of good practice	16
12.2 Appendix 2 - List of Hardware	17
12.3 Appendix 3 - Declaration	18

1. Introduction

Staffordshire County Council's (SCC's) intentions for publishing an ICT Acceptable Use Policy are not to impose restrictions that are contrary to the Council's established culture of openness, trust and integrity. SCC is committed to protecting its users, partners, contractors and the County Council from illegal or damaging actions by individuals, either knowingly or unknowingly.

Systems, including but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, are the property of SCC. These systems are to be used for purposes in serving the interests of SCC, our partners and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every SCC employee and affiliate who deals with information and/or information systems. It is the responsibility of every user of SCC systems to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to provide a framework for the acceptable use of computer systems within SCC. These rules are in place to protect the user and SCC. Inappropriate use exposes SCC and users to risks including virus attacks, compromise of network systems & services, and legal issues.

3. Scope

This policy applies to employees, elected Members, contractors, consultants, temporary staff, and other workers at SCC, including all personnel affiliated with third parties. This policy applies to all services, systems and equipment that is owned or leased by SCC. There is a separate policy to cover mobile devices and remote working, see item 12 related documents location. The ICT Acceptable Use policy applies whether or not the systems are used outside office hours or outside the office.

4. Reporting Security Incidents

If you become aware of a possible or suspected security-related issue, whether it relates to a problem with a computer or an individual's actions then please report it immediately and in confidence to the Staffordshire ICT Service Desk on 01785 278000 or if appropriate to your Line Manager.

The ICT Service Desk will instruct you on the correct procedures which you must take immediately to preserve the incident scene. If it is a virus-related incident then see

section 5.3 below for instructions. The following procedures will be given to you with regard to any computer equipment believed to be involved in the security incident:

Avoid any involvement with computer equipment which may affect the current state. This means you **must not**:

- touch the keyboard or mouse;
- press the reset button;
- turn on any equipment;
- disconnect any leads; (unless the PC is infected with a virus or malware)
- attempt to shut down the machine in any way.

The incident scene must be constantly monitored and protected to safeguard evidence. This responsibility may fall upon your present line manager.

The ICT Service Desk will immediately contact the Information Security Team, who will make direct contact with you.

If you do not feel that you can report the issue to your line manager or if the issue is of a sensitive or confidential nature then you can contact the Information Security Team by the confidential email address: ictsecuritysupport@staffordshire.gov.uk

5. General Use and Ownership

5.1 Hardware

All assets including but not limited to the items in Appendix 2 are the property of SCC and must not be used by unauthorised persons including family members:

You must not

- connect privately owned ICT hardware, including but not limited to those listed in Appendix 2, to any SCC ICT equipment without permission from the Information Security Team;
- modify or expose the inner workings of or in any other way tamper with any item of SCC ICT Hardware;
- relocate any item of SCC ICT Hardware, other than items such as laptop computers that are intended to be portable without first consulting the ICT Service Desk.

Only SCC ICT Support Officers or approved contractors can service, modify, add or remove components or in any other way alter the ICT equipment belonging to SCC.

5.2 Software

Software can only be installed, configured or uninstalled on SCC owned hardware by SCC ICT Support Officers. Administrative rights must only be used if a user has been authorised by Staffordshire ICT. Users must not make configuration changes.

You must not

- make unauthorised copies of copyrighted software, except as permitted by law or the owner of the copyright;
- download or install software from the Internet including shareware, music and other audio files, games and screensavers.

The ICT Service Desk should be contacted if you have queries regarding the restrictions and to obtain assistance with the removal of unauthorised software and files.

If you have any queries concerning the use and licensing of software then please contact the Staffordshire ICT Asset Manager 01785 27(4503) or the ICT Service Desk on 01785 278000.

For more information on acceptable software use see the Software Standards Policy <http://www.intra.staffordshire.gov.uk/ict/Standards>

5.3 Computer Viruses

It is a crime to deliberately or recklessly introduce a computer virus, under the Computer Misuse Act 1990. You must not use our e-mail and internet facilities for

- intentionally accessing or transmitting computer viruses or other damaging software;
- intentionally accessing or transmitting information about or software designed for, creating computer viruses.

We have an anti-virus protection system, in place throughout the Council. You must not e-mail material that has not been scanned against viruses to other users in our network. If you find a virus, or suspect that your PC has one, you must immediately disconnect from the network, stop using the computer and tell the ICT Service Desk.

You must always follow the instructions that the ICT Service Desk or ICT Desktop Support Team give you about virus attacks.

When new versions of the anti-virus software are released computers attached to the corporate network will be updated automatically.

Remote and Laptop users must ensure that their computers are connected to the corporate network at least once every two weeks so that the Anti-Virus software can be updated.

You must ensure that the anti-virus protection on your equipment is not disabled.

If you are not sure how to use the virus protection system, you must obtain advice from ICT Service Desk.

5.4 Transfer or Storage of Data

You must be aware that the data you create with SCC equipment and systems remains the property of SCC.

You must

- keep all business-related data on the SCC network and not on the hard drive of your PC. Data that is stored on the SCC network is backed up on a regular basis;
- ensure that you regularly check the files that you have stored on the SCC network and delete those that are no longer required;
- lock sensitive data (hard copy and disks) away when not in use;
- ensure that sensitive data, both paper-based and electronic is disposed of properly – shred hardcopies and destroy disks.

You must not

- store personal data (non SCC work) files on the SCC network or storage media including the personal home (H or U) drive;
- copy files that are accessible centrally on the SCC network onto your personal home (H or U) drive on the network unless for amendment after which they must be deleted from the home (H or U) drive. Wherever possible, work must be kept on shared network drives and not on your home (H or U) drives;
- attempt to access any data or programs within the SCC network that you do not have authorisation or the explicit consent of the owner of the data or program to do so. If you intentionally access a computer system or information without permission, then you are breaking the law under the Computer Misuse Act 1990;
- send business-related sensitive/personal information via e-mail externally without suitable security measures being applied. Further advice can be sought from the ICT Service Desk 01785 278000.

6. Internet and Email Use

6.1 Access to Email and Internet Services

Your connection to e-mail or the internet will have been authorised (in writing or in electronic form) by: your Head of Service or Business Unit Manager (if you are staff); or the Chief Executive's Office (if you are an elected Member).

Our e-mail and internet facilities are for business use but we will allow staff and elected Members to use them for private purposes. The personal use access will be limited for staff to an hour per day and must only be used outside work time. Access to specific non-business related sites may be restricted during certain times of the day to prevent an adverse impact on business use.

When you connect to the corporate network a message displays asking you to confirm that you understand and accept the terms and conditions of use for e-mail and Internet services. The declaration in Appendix 3 contains the details of what you are agreeing to as a condition of use. If you do not understand or accept the terms and conditions of use you should not proceed with connecting to the network and inform your line manager.

You must not use for business purposes other internet-based e-mail accounts e.g. Hotmail and Yahoo. Any e-mail sent to internet-based e-mail accounts is not secure.

You must not make use of instant messaging or peer-to-peer file sharing.

If there is a genuine business requirement to use either of the above it must be authorised first by the Deputy Corporate Director (Information). Requests for use should be forwarded to the Information Security Team lctsecurityqueries@staffordshire.gov.uk.

User accounts on the Exchange mail service have a limit on storage capacity. You must manage the mailbox account by deleting mail that is no longer required from the Inbox, Sent Items and Deleted Items folders. If the mail is business related before deletion consideration must be given to any relevant information retention policies.

<http://www.staffordshire.gov.uk/yourcouncil/dataprotectionandfreedomofinformation/recordsmanagement/>

If your mailbox reaches the limit mail can still be received but the ability to send messages will be suspended. Mail can only then be sent once the mailbox is reduced below the limit. For advice and further assistance contact the ICT Service Desk.

When you connect to the corporate network you will be reminded that in proceeding you understand and accept the terms and conditions of the policies. In addition, when revisions are made to the policy you will be asked to read the policy and accept the terms and conditions. All internet and e-mail activity is logged for audit and performance

monitoring purposes and the account holder is responsible for all activity logged against that account.

You must not attempt to connect to the network using another users account details.

You must:

- use Ctrl-Alt-Del keys to lock your PC when leaving your desk;
- enable password protected screensavers to protect screen content;

6.2 Prohibited use

The following section details prohibited use both in business and personal use

You must not use, or try to use, our e-mail and internet facilities to create, distribute or display in any form any material that is or may be considered to be illegal, offensive or unacceptable under our rules and policies. It is impossible to give a complete list of what is considered offensive or unacceptable, but the following are included (and in some cases may also be illegal). Anything that:

- is pornographic or obscene, or includes any form of sexually explicit humour;
- is intimidating, discriminatory (for example, racist, sexist or homophobic) or breaks our anti-harassment and equal opportunities policies in any other way;
- is defamatory, encourages violence or strong feelings;
- is hateful;
- is fraudulent;
- shows or encourages violence or criminal acts;
- may give SCC a bad name; or
- is a deliberate harmful attack on systems we use, own or manage.

You must not use the e-mail or internet facilities for time-wasting activities, such as chain letters, or for sending private e-mails to everyone on the global address list.

When using SCC e-mail facilities for private purposes to reduce the likelihood of SCC being targeted by spam, phishing or potential malicious activities you must not use your SCC email address when buying personal goods online.

You must not make personal use of internet discussion groups, chat rooms or forums.

You must not use or try to use our facilities for:

- on-line gambling;
- Carrying out a personal business operation for profit or charity;

- Accessing, without permission, any e-mail that is intended for another user or an e-mail account of another user. If legitimate access is required contact the ICT Service Desk 01785 278000.

For more detail on what is and is not allowed refer to the internet Blocking Policy on the corporate intranet.

Unless performing a legitimate test as part of your normal job function and with authorisation of senior management, you must not use or try to use our facilities for

- accessing or transmitting information about, or software designed for, breaking through security controls on any system;
- breaking through security controls to gain access on any system.

6.3 Copyright

6.3.1 Copyright Documents

You must know that copyright applies to most documents automatically and that if you break the copyright rules you may be committing a criminal offence. However, a large amount of copyright material is put onto the internet with the expectation that it will be copied and distributed. The only sensible approach is to consider whether the author or owner of what is being transmitted is likely to object. For example, you can normally pass on an e-mail that contains government advice but you must get permission before you pass on an e-mail containing some technical advice from a commercial consultant.

6.3.2 Copyright Emails

Copyright protection also applies to e-mails. For example, unlawfully scanning a chapter from a textbook and distributing the resulting file by e-mail breaks the author's copyright just as much as photocopying the chapter and sending the copies by post.

6.3.3 Copyright Software

Computer software has copyright protection in the same way as written documents. You must not transmit copyrighted software from your computer to the internet, or allow any other person to access it on their computer through the internet.

6.4 Publishing information

6.4.1 Information on the internet

The appropriate Head of Service or Business Unit Manager or, if you are an elected Member, the Chief Executive's Office, must authorise any information that is to be published on the internet. We will not allow unauthorised publishing on our facilities. The Chief Executive's Office is responsible for managing our website.

6.4.2 Transmitting Information

You must make sure that any advice or information that you transmit by e-mail or over the internet (as with other forms of correspondence) does not contradict our policies or interests. If you are in any doubt, you must ask your Head of Service or Business Unit Manager.

6.5 Confidential or sensitive information

6.5.1 Data Protection Act

You must not break the conditions of the Data Protection Act 1998 when you use the e-mail services or the internet for transmitting information. If you need any more advice about these conditions, you should contact your directorate's Data Protection Representative or the Chief Executive's Office if you are an elected Member.

6.5.2 Sending Confidential or Sensitive Information via Email

The internet e-mail facility is not a secure way of transmitting confidential, sensitive or legally privileged information. Internet e-mail is as insecure as a postcard that you send through the normal post. So, you must make sure that the internet e-mail is suitable for transmitting the information. If you need to send information that is confidential, sensitive or legally privileged, e.g. Social Care and Health reports on vulnerable children or details of project tender submissions, take advice from Staffordshire ICT Information Security staff about special security measures (such as encryption) that you must use. If you allow anyone to see this type of information without permission, you may be breaking the law.

6.5.3 Email Disclaimer

The system will automatically attach the following disclaimer to e-mails that you transmit over the internet (i.e. external e-mails).

Disclaimer:

This email (including any attachments) is only for the person or organisation it is addressed to. If you are not the intended recipient you must let me know immediately and then delete this email. If you use this email without permission, or if you allow anyone else to see, copy or distribute the email, or if you do, or don't do something because you have read this email, you may be breaking the law.

Liability cannot be accepted for any loss or damage arising from this email (or any attachments) or from incompatible scripts or any virus transmitted.

Emails and attachments sent to or received from staff and elected Members may be monitored and read and the right is reserved to reject or return or delete any which are considered to be inappropriate or unsuitable.

6.6 Bulletin board

There is a 'bulletin board' (an electronic notice board) on our intranet for social and personal use. The conditions of use in this policy also apply to the bulletin board. We are not responsible for the content of any material included in the bulletin board or for anything users do because of the material.

6.7 Monitoring and Recording

6.7.1 Network Monitoring

For security, capacity planning and network performance purposes, authorised individuals within SCC may monitor equipment, systems and network traffic at any time. SCC reserves the right to audit networks and systems on a periodic basis to ensure compliance with SCC policies.

6.7.2 Email Monitoring

We have the right to monitor and inspect:

- any e-mails sent using our systems, both to internal and external addresses;
- any e-mails received using our systems;
- any material downloaded from the internet using our systems; and
- any electronic material stored on our systems.

We own our e-mail system which means that we also own all copies of messages created, received or stored on the systems. This means that nothing will be private, even if marked as "private" and/or "confidential" or with any similar wording.

For external e-mail users a warning of the monitoring policy is included in our terms and conditions on Staffordshire Web.

This monitoring will make sure that this policy is effective and that our users are keeping to it. It also makes sure that our computer systems are working properly.

6.7.3 Internet Usage Monitoring

We centrally record how our internet facilities (provided by Staffordshire ICT) are used. We regularly inspect the records to check for any access or attempted access to internet sites that are not allowed under the conditions of the ICT Acceptable Use Policy. We also monitor the records to make sure that our business is not affected by excessive personal internet use or by unauthorised internet use.

We have the right to monitor and inspect any internet use for any purpose we deem necessary. There can be no expectation that the use of our systems for looking at the internet sites will be private.

If you access a prohibited internet site unintentionally, you must break the connection immediately and report it to your Head of Service or Business Unit Manager or, if you are an elected Member, to the Chief Executive's Office. If you do not do this, we may take action against you.

7. If You Break This Policy

If you break any of the rules on purpose, we may:

- withdraw your access to the e-mail or internet facilities, temporarily or permanently;
- take disciplinary action against you (if you are staff);
- refer the matter to the appropriate ethics or standards committee (if you are an elected Member);
- bring criminal proceedings against you, or ask the police or other relevant body to, if the matter is also a criminal offence; or
- do a combination of these things.

If you misuse our systems, we could take disciplinary action against you which may lead to you being dismissed. Serious cases will result in you being dismissed for gross misconduct.

If you try to damage, defeat or deceive one of our security facilities, we will take disciplinary action against you.

If you suspect someone has broken this policy, you must report this to the line manager and Staffordshire ICT Information Security staff. If a problem is discovered at an early stage, we can usually deal with it at a local level. However, if the case is more serious, the line manager or Staffordshire ICT Information Security staff should report it to the Head of Service. In certain circumstances, we may need to carry out an investigation and internal audit.

If you find or suspect anyone of using the computer system illegally or unethically, you should report it to your Corporate Director.

8. Further Guidance or Training

If there is anything within this policy that you are unsure of and wish clarification then you can contact the Information Security team on 01785 278120/8128/8090 or email ictsecurityqueries@staffordshire.gov.uk.

If you feel that you require further training on internet and email usage then you should speak to your line manager.

9. Glossary

Data: A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing.

Systems: Includes but is not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing

SCC: Staffordshire County Council

SICT: Staffordshire Information and Communications Technology

Bulletin board: an electronic notice board on the SCC intranet.

Handheld Devices: An electronic device which holds electronic data these can include: Blackberries and PDA's (Personal Digital Assistant) .

10. Points of Contact

Contact Area	Details
Information Security	ictsecurityqueries@staffordshire.gov.uk (01785) 278120 / 8128/ 8090
Information Security (confidential)	ictsecuritysupport@staffordshire.gov.uk (01785) 278120 / 8128 / 8090
ICT Service Desk	ict@staffordshire.gov.uk (01785 278000)

11. Related document locations

Document name	Location
Corporate Information Security Policy	http://www.intra.staffordshire.gov.uk/it/policies/CorporateInformationSecurityPolicy.htm
Password Policy	http://www.intra.staffordshire.gov.uk/it/policies/Staffordshire+Password+Policy.htm
Internet Blocking Policy	
Mobile Device and Remote Working Policy.	

12. Appendices

12.1 Appendix 1 - Email code of good practice

Email code of good practice

The following guidelines (some of which also apply to other forms of correspondence) tell you what is and what is not good practice when you use internal or internet e-mail services.

You **should**:

- check your e-mail inbox for new messages every working day;
- reply to e-mails in line with the Council's standards for dealing with correspondence;
- only send information in an e-mail that you would be happy sending in an open memo through the internal post system;
- check the message and think how the person will react to it, or how you would feel if you received it, before you send it;
- make sure you use correct and up-to-date e-mail addresses;
- attach a signature to your e-mails giving your name, job title and contact details, preferably in rich text format (RTF);
- file mail when you have dealt with it and delete any items that you do not need to keep; and
- use the Outlook 'Out of Office' facility (in the 'Tools' menu) to tell internal e-mail senders when you will read their message, or use the 'delegate' or 'permissions' facilities so another authorised person can read and deal with new e-mails while you are out.

You **should not**:

- use e-mail to manage staff where face-to-face discussion is more appropriate;
- create wide-distribution e-mails (for example, to addressees throughout the world) unless this form of communication is vital;
- send large file attachments to e-mails to many addressees;
- print out messages you receive or send unless you need a hard copy;
- retain e-mails for longer than is necessary – if the email contains personal data give consideration to Principle 5 of the Data Protection Act;
- send an e-mail that contains indecent inappropriate, offensive or profane content;
- send an e-mail that the person who receives it will think is a waste of resources; or
- use jargon, abbreviations or symbols if the person who receives the e-mail may not understand them.

12.2 Appendix 2 - List of Hardware

1. Cables
2. Desktop Personal Computers
3. Digital Cameras
4. Handheld Devices
5. Headphones
6. Keyboards
7. Laptop or Notebook Personal Computers
8. LCD Projectors
9. Mice
10. Mobile Phones
11. Modems
12. Monitors
13. Network Cabinets
14. Cables
15. Printers
16. Scanners
17. Servers
18. Speakers
19. Switches and Routers
20. Tablet Personal Computers
21. USB Storage Devices
22. Video Conferencing Equipment
23. Video Recorders
24. Wireless
25. MP3 players

12.3 Appendix 3 - Declaration



Declaration for Users of SCC Systems including Members and contractors.

This declaration expands on the terms and conditions you accept whenever you connect to the corporate network and use the e-mail and internet services.

Declaration

I confirm that, as an authorised user of the County Council's systems, I have read, understood and accepted all of the conditions in the Acceptable Use Policy.

I also fully accept that if I deliberately break any conditions in the policy, the County Council may:

- withdraw my access to the e-mail, internet facilities or any other systems temporarily or permanently;
- take disciplinary action against me (if I am staff);
- refer the matter to the appropriate ethics or standards committee (if I am an elected member);
- begin criminal proceedings against me, if the matter is also a criminal offence; or
- undertake a combination of these things.