Staffordshire County Council

Acceptable Use Policy

Document Management

Document Disclaimer

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

Document Owner

This document is produced and owned by Staffordshire County Council (SCC). It is the responsibility of the Information Governance Unit 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	IGU ICT Legal

Version Control

Version	Author(s)	Reason for Change	Date
0.1	Information Governance Unit	Initial draft for distribution and review comments	July 12
0.2	Information Governance Unit	Head of Information Governance final approval.	Dec 12
0.3	Information Governance Unit	Policy review.	July 14
0.4	Information Governance Unit	Policy Review	Apr 15

Approvals

Version	Name	Position	Date Approved
0.2	Philip Jones	Head of Information Governance	Dec 12
0.3	Philip Jones	Head of Information Governance	Jul 14
0.4	Philip Jones	Head of Information Governance	Apr 15

Contents

INTRODUCTION

Staffordshire County Council recognises that information technology and communication systems play an essential role in enabling greater efficiency and can significantly improve business performance.

To operate effectively within the Council, these technologies and systems rely on employees and other Council ICT users observing relevant policies, procedures and best practice guidelines.

Whenever you log on to the network the following message appears:

The County Council's Information and ICT equipment (including mobile devices), email, network, and internet services may only be used in accordance with the County Council's Information Security, Acceptable Use Policies and associated guidance which are available on the Intranet. It is your responsibility to read and understand the contents of these policies and by proceeding beyond this point you are accepting the terms and conditions of all relevant policies. If you do not abide by these terms and conditions, your access to the system(s) may be restricted or removed and you may be subject to disciplinary action by the County Council.

Internet, network and email use is logged for audit and performance monitoring purposes including inappropriate use and you are responsible for all activity logged against your network account. All passwords should remain confidential and should not be shared with others, whether verbally or otherwise.

By progressing beyond this point you are agreeing/accepting the above.

You are agreeing to abide by the entire contents of this policy when you connect to the network. You must make sure that you understand the contents of this policy and what is expected of you.

This policy should be read in conjunction with the Corporate Information Security Policy, the Code of Confidentiality and the Standard of Conduct for Employees.

It is the responsibility of all Council employees to comply with this policy and be familiar with its content. Furthermore, line managers/senior officers, employees and contractors/external partners have specific responsibilities:

Line Managers/Senior Officers

Line Managers/Senior Officers are responsible for ensuring that employees and other users of the Council's ICT facilities within their own services are informed of and work in a manner that is consistent with the principles outlined in this policy.

Members and Employees

It is the responsibility of all Members and employees to ensure that they have read, understood and observe this policy and any other relevant associated codes of practice and guidance documents.

Members and employees **must** fully understand that all systems and services are provided as business tools and that there is no guaranteed individual right to privacy.

Contractors/External Partners

Contractors/External Partners must be made aware of this policy and any relevant codes of practice and guidance. Appropriate ICT access will be provided where necessary to allow work to be carried out as set down by the Council but only once the Third Party Access Agreement has been signed and returned prior to work starting.

Reporting Information Security Incidents

It is extremely important that in circumstances where there has been an information security breach, the Head of Information Governance is made aware immediately so that the impact of the breach can be minimised. It is a disciplinary offence to not report or withhold information regarding a breach or a suspected breach.

SECTION ONE – INFORMATION SECURITY

1.1 Password Protection.

All employees are directly accountable for all ICT activity associated with their user account. It is the responsibility of the user to protect their password.

- You must not tell anyone your password.
- You must not write down your password.
- You must not ask anyone for their password.
- You must not log onto the network as another user.
- You must not allow another user to use any device whilst you are logged onto to it.

Further guidance on password security can be found on the intranet

1.2 Authorised Information Access.

The ability to access information (Hardcopy or Softcopy) or systems containing information is not the same as having the authorisation to do so.

If you are unsure that you are authorised to access particular information or systems you must check with the Data Owner.

The Data Owner is the person within the service area who has been assigned the role to manage the handling of and access to specific information and information systems.

- You must not access or attempt to access information or systems containing information that you do not need in order to carry out your role.
- You must not facilitate or attempt to facilitate access for anyone else who is not authorised to access specific information or information systems

1.3. Responsible Email, Internet and Lync Use.

All access to our email, internet and Lync systems is monitored and all activity is recorded. There can be no expectation of privacy. You must only use our email, internet and Lync systems in accordance with the Email, Internet and Lync guidance.

All terms entered into internet search engines are recorded. For investigation purposes content resulting from a search term will be treated as having been accessed irrespective of whether it was blocked by the corporate internet filter. Similarly email will be treated as having been delivered to the intended recipient irrespective of whether it was blocked by the corporate email filter.

- Under the Freedom of Information Act 2000, email communications fall within the definition of 'recorded information' and the Council may be obliged to provide these if requested. All employees must ensure that the content of their emails is business related and the language used is in no way discriminatory or defamatory.

- You must not email SCC personal data to your own personal internet based email account.

- You must not access or attempt to access illegal or offensive content on the internet.

- You must not or attempt to distribute illegal or offensive content using our ICT systems.

- You must not upload SCC data to any Personal Network storage sites such as Dropbox or WeTransfer.

- The Council will not be responsible for any damage, distress or loss a user may suffer, including the loss of personal data or losses sustained in any on-line financial transaction whilst using the Council facilities for personal reasons. The County Council email addresses must not be used for on-line shopping and banking transactions.

1.4. ICT System Protection.

SCC has in place a number of ICT Security systems to protect the SCC network from malicious software. Malicious software if it infected our network could result in loss of service and/or unauthorised external access or disclosure of SCC Information.

- You must not, nor attempt to, disable the Anti-Virus protection on your device(s).

- You must not, nor attempt to, access or transmit information about software designed for breaking through security controls on any system.

- You must not, nor attempt to, intentionally access or transmit information about computer viruses' or other malicious software.

- You must not, nor attempt to, access or transmit information about software designed for creating malicious software.

- You must not connect personal devices to the network without explicit permission from senior management and ICT. If permission is received then you must ensure that ICT inspect the device before it is connected.

- You must not, nor attempt to, bypass or deceive any ICT security systems that are in place including internet and email systems.

- You must not, nor attempt to, download or install software from the Internet including shareware, music, games, wallpapers etc.

- You must not leave your PC without first locking your computer screen so that it cannot be accessed by someone else in your absence whilst you are logged on.

1.5. ICT Equipment Protection.

All SCC ICT equipment must only be used for work purposes. Once you take possession of the equipment you are directly responsible for the security of the equipment. Should the equipment be damaged, lost or stolen you will have to account for your actions.

- If you have a mobile device you must connect it every two weeks to the network to ensure that it has the most up to date anti-virus software and security patches installed.

- SCC ICT equipment must only be used by SCC employees and authorised third parties. You must not allow unauthorised users including family and friends to use your SCC ICT equipment.

- You must ensure that any SCC work mobile devices are encrypted.

- Laptops and smartphones used for SCC business must be purchased through Staffordshire ICT.

1.6. Security of Records

You are directly responsible for the security of SCC data and are accountable for your actions if:

- You access it from non SCC equipment e.g. through Citrix or Outlook Web Access (OWA) at home.

- You take it off site in paper form, or on storage devices such as USB pens or media CDs.

- You transfer it to any external agency you are still responsible for the security of the data, during the data transit and once it is with the third party.

Therefore:

- You must ensure when accessing SCC data at home that no-one else including friends or family can access the data or be able to view it.

- You must only take paper documents containing sensitive personal data with the explicit permission of your manager.

- You must keep a record of the request, the manager authorising, the documents taken off site, the location where they will be kept and the duration that they will be held off site.

- You must never leave paper records containing personal data unattended at any time even when working at home.

- You must never take paper records containing personal data into public buildings if not directly for work purposes.

- You must store the paper records in a secure lockable storage cupboard or cabinet when not in use.

- You must not store SCC data on personal devices including home PCs, laptops or smartphones.

If you are unsure about the storage or transfer of data you are advised to contact the Information Governance Unit. Further guidance on working from home securely can be found here.

SECTION TWO – IT HARDWARE, SOFTWARE & NETWORK ACCESS

2.1 Supply and Use of ICT Hardware

- Hardware is the physical equipment used in a computer system. The Council will issue ICT users with equipment to enable access to the ICT network and services. This will include, as appropriate, a desktop/laptop PC or THIN client (Citrix) device together with associated keyboard, mouse, screen, docking station, disk drives, printers, memory and mobile devices such as a smart phone or other approved hand held devices.

- With the exception of portable devices, such as laptops and smart phones, equipment should not be disconnected, moved or modified in any way without prior discussion with ICT services.

- Equipment which is not owned and supplied by the Council should not be attached to the Council network. Devices which are not owned and supplied by the Council should not be attached to Council ICT equipment. However, if there is a business need to use privately owned devices authorisation and justification must be sent by an appropriate manager to Staffordshire ICT for consideration and approval. You must not use the council's network storage for personal use.

- ICT are responsible for the selection of appropriate computer equipment. Through centralisation, equipment is acquired at competitive prices and compatibility is maintained. If an employee needs to use a computer or change the use of their present machine, contact your Line Manager to discuss your service needs.

- Computer equipment should be disposed of safely and appropriately and should not be disposed of by an employee/user themselves. A call should be raised through the self-service portal detailing the equipment to be disposed of. ICT will then arrange to dispose of the equipment in line with SCC policy.

- All County council mobile devices must be encrypted even if they do not contain restricted or confidential data. Laptops and tablets will be encrypted automatically providing they have been connected to the corporate network. USB memory sticks must also be encrypted using the software provided by Staffordshire ICT. You must speak to ICT Service Desk for up to date information on encryption solutions.

2.2 Supply and Use of ICT Software

- Only approved software required to support business functions and applications will be installed on council hardware. All such software will be installed by ICT. Employees or any other users of the Council's ICT equipment must not install, move or copy software, change any system files or duplicate copyright document images.

- No Council owned software may be installed on personally owned equipment unless the licence agreement specifically permits this.

- A standard set of end user computer software products are available, chosen to provide a balance and up-to-date coverage of most business needs. It is continually reviewed to keep in step with advances in technology.

- If a business-specific application is needed, contact your ICT Business Account Manager, who will ensure that all technical considerations relating to your requirements and underlying Council systems are addressed.

- All software used on Council ICT equipment must be authorised and acquired legally. ICT will hold and maintain licences for standard desktop system and application software.

- Council print\scan\copy\secure file transfer facilities must not be used for personal purposes without permission from a line manager/senior officer.

2.3 Wireless Access

Corporate Wireless Access will be configured as standard by Staffordshire ICT for use within corporate buildings. Requests should be made by raising a call via the ICT Self Service Portal with the appropriate authorisation if any member of staff or visitor requires access to the guest wireless network. Access to the Guest wireless network is for business use only and must not be used for non-work activities. Logs of guest wireless use are maintained and are routinely monitored. Any suspected personal use of the Guest Wireless network will be investigated and if appropriate referred to HR.

We will allow you to connect your corporate laptop to your home broadband. .

Public Access Hotspots are not secure and pose a risk. If you have a continual need to use Public hotspots as a means to connect remotely to the corporate network you should use VPN access instead of Citrix. To arrange for your laptop to

be configured for VPN access please raise a Service Desk call via the Self Service portal.

2.4 Email

- 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. Emails will be automatically archived by Enterprise Vault if they are older than 3 months or if free space falls below 10%. If the email is business related, before deletion consideration must be given to any relevant information retention policies.

- 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, you should raise a Service Desk call via the Self service portal.

2.5 Council Telephone Systems – General Principles of Use

- All telephones and mobile handsets are provided for use in support of the Council's business. Before making a personal call, seek permission from your Line Manager/Senior Officer.

- You must not take your works mobile phone abroad without permission **under any circumstances**.

- Employees must not try to use or let anyone else use Council supplied telephone equipment for:

    - Anything that is illegal or immoral

    - Making offensive or threatening calls

    - Making calls which can be construed to constitute harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin or political beliefs

    - Unreasonable personal use

    - Use in relation to any other business owned or operated by the employee.

- Telephone usage is subject to routine monitoring and auditing. All outgoing telephone calls are detailed on telephone bills and unexpected peaks and excessive usage may be investigated in conjunction with the relevant line manager/senior officer. In order to ensure continuity of service, facilities such as voicemail may be required to be monitored by a line manager/senior officer or other colleagues where an employee is absent from the workplace e.g. sickness absence, period of annual leave.

2.6 Mobile Communications Devices

- Mobile phone and any other mobile communications devices are provided for use while on Council business. Mobile telephone calls are often more expensive than fixed line calls so should be kept as short as is reasonably possible. They should only be used where no fixed alternative telephone line is available or where the use of a fixed line is inappropriate.

- Mobile devices are the property of Staffordshire County Council and are issued for legitimate Council business purposes only.

- Communications devices capable of transmitting and receiving data information, such as smart phones and tablets, must only be used for the purposes for which they were supplied. They must not be connected to third party networks or hardware which is not Council owned. This will ensure that these devices remain free of viruses and other malicious software which may be transmitted on unknown networks. If it is essential for operational reasons to connect your smart phone or tablet to a third party network or hardware you must seek ICT guidance by raising a support call through the Self Service portal before connecting.

2.7 Voicemail

- Employees are reminded that voicemail messages are Council records. The Council reserves the right to access the contents of these messages where there is reasonable cause to do so.

- Employees are responsible for maintaining the security of their voice mail. Employees should take precautions to prevent unauthorised access to their mailbox by ensuring their access pin code number is not divulged. Unauthorised entry to another employee's voice mailbox is not permitted and may result in disciplinary action.

- Shared voicemail accounts may be set up for certain services. It is the responsibility of the manager of any service with a shared mailbox to ensure the management and security of shared mailboxes.

- Employees are responsible for maintaining their mailboxes. Voicemail should normally be checked on a daily basis. Voicemail messages should not be stored for longer than is necessary. Mailbox greetings should be kept current, accurate and relevant.

2.8 Health & Safety

- All ICT facilities and telephone devices must be used with care and, when using a mobile, in line with the legal requirements for hands-free devices when driving. For further guidance speak to a member of the Health & Safety Team.

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.

Name:

Signature:

Date: