Staffordshire County Council

Acceptable Use Policy

Written by: SCC

Review Committee: Finance & Resource

Date Approved: June 2019

Review Date: June 2020

Responsible for Day to Day Management: PC

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

Change Approval

The Acceptable Use Policy is reviewed regularly and amended as necessary. The Corporate Governance Working Group will agree significant changes to the policy.

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.

This policy is written in three main sections and refers to all ICT systems including GCSx and PSN.

a) The first section relates to Information Security Principles which **must** be adhered to – not complying with these may result in disciplinary action being taken against you up to and including dismissal.

b) The second section relates to your use of the IT equipment and systems with which you are supplied as part of your employment with the Council.

c) The final section relates to Information Governance Principles – these **should** be adhered to and form the basis of your working practices. Failure to comply with these working practices may result in the Information Governance Team investigating the incident.
Whenever you log on to the network the following message appears:

The County Council's 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 IT Security Policy, the Code of Confidentiality and the Code 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 Internet and Email Use.

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

- You must not email SCC personal data to internet based email accounts without permission.
- 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.
- Further guidance on internet and email use can be found on the intranet

1.3.1 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.

- **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.
- **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.

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 virus scan 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.

1.5. ICT Equipment Protection.

All SCC ICT equipment must only be used for work purposes. Once a user takes possession of the equipment they are directly responsible for the security of the equipment. Should the equipment be damaged, lost or stolen the user will have to account for their 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 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 devices that hold personal data are encrypted.

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 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

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.

- 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 placed with ICT Service Desk (ext 27 8000) 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.

- No restricted or confidential data must leave the County Council unless it is encrypted

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 the appropriate Line Manager to discuss this requirement. ICT 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. This is an individual and service responsibility. 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.

- 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.

2.3 Wireless Access

Corporate Wireless Access will be configured as standard by Staffordshire ICT for use within corporate buildings. Requests should be made with the appropriate authorisation if any member of staff or visitor requires access to the guest wireless network.

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. If the mail is business related, before deletion consideration must be given to any relevant information retention policies. Further information can be obtained from the Records Management pages of the intranet.

- 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 (Ext 27 8000)

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. Where personal calls are made provision exists for these to be recorded as such and costs recovered. Before making a personal call, seek permission from your Line Manager/Senior Officer.

- 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. Permission is granted for a mobile device to be used to make a personal call or send a personal text message **provided** all personal use is identified and paid for and the device is issued for your own use only.

- Communications devices capable of transmitting and receiving data information, such a smart phones, 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.

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.

SECTION THREE – INFORMATION GOVERNANCE PRINCIPLES

3.1 The Principles

The Council is registered under the Data Protection Act 1998. Employees should be aware of their responsibilities when processing personal and sensitive data of any living individual (including name, addresses and telephone numbers).

- **Personal Use/Right to Privacy**

  Staff must be aware that when using the Council's ICT systems for personal use, there is no automatic right to privacy. The ICT systems are monitored and misuse will be identified and acted upon.

- **Correspondence**

  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. This includes emails relating to trade union activities and emails to and from trade union representatives and their members.

3.2 Expected Behaviour

- It is important to understand that the Council owns and is liable not only for the equipment, hardware and software but also for any information, including emails sent and received and all internet/intranet pages generated or stored on the Council's ICT equipment.

- There are three key points to remember when upholding the privacy of data

  1. *Responsibility*
     It is necessary for the Council to process personal data of its customers and employees in order to provide successful services. We are trusted to look after this information and it is everybody's responsibility to ensure that we are compliant with appropriate Data Privacy laws.

  2. *Reputation*
     Protecting the Council's reputation is of significant importance and one way in which we can ensure that we do so is by processing

personal data carefully and securely. We rely on the actions of our employees in order to maintain this standard.

3. *Respect*
Give appropriate consideration to what you say and to whom. Customers and employees provide information to us for particular purposes and we must respect that in order to maintain their trust.

- Precautions should be taken to avoid revealing confidential information to those within the immediate vicinity. This is especially important in open plan offices and public areas. Employees are encouraged to use smaller offices – if available – for making/taking calls of a confidential nature.

- Confidential information must never be left as a message on an answer phone. Before discussing confidential information with another person their identity and location must be confirmed.

- Do not access or attempt to access any data on Council systems unless it is directly related to your role. Having the ability to access information is not the same thing as being authorised to access it.

- All staff must assign a security level to data in accordance with the Protective Marking Scheme. In order to mitigate the risk of data loss the rules relating to the security level must be followed.

- It is important that all staff remember to check the contents of all correspondence before sending by email, post or any other means to ensure addresses are accurate and enclosures are relevant.

- You are responsible for any data that you send to print. Ensure all data is removed from the printer and any originals removed after photocopying or scanning. You must also check that you have not collected any data that has been copied, printed or scanned by another member of staff.

3.2.1 Personal Use of ICT

- Employees studying for a work-related qualification with Council support may use Council facilities to prepare study material. However, this must be done in break periods unless otherwise approved by a senior manager. No SCC personal or sensitive data may be used to prepare, research, or produce material in connection with qualifications without the explicit consent of the relevant Senior Information Risk Officer (SIRO).

- The Council's ICT equipment and facilities, including the internet, may not be used to prepare, research or produce material in connection with a private business or any area which may be deemed as a conflict of interest as detailed

in the Code of Conduct for Employees. If in doubt, further clarification must be sought from the employee's senior manager.

- Personal use of the Council ICT facilities is a privilege and not a right. Limited use of Council intranet and the internet for personal purposes is permitted for employees. However, this **must not** take place during an employee's recorded working hours. You must not use the council's network storage for personal use.

3.3 Governance Standards

- Extreme care should be taken when sending out confidential data to either employees or members of the public. Name and addresses should be double-checked and the envelope marked "Strictly Private & Confidential".

- Confidential data must not be sent via email unless the current requirements of the Protective Marking Scheme are met. For advice on options for encryption contact the ICT Service Desk (☎ 278000).

- For the limited number of staff using GCSx accounts, additional and separate guidance is provided. This should be read prior to using a GCSx account.

- Council owned data must not be transferred from Council systems and stored in an unsecured format. Advice on encrypting data to be transferred can be sought from the ICT Service Desk (☎ 278000).

- Do not transfer personal data outside Council systems without seeking advice from the Information Governance Unit.

- If an employee needs to work on data away from the office, advice on the best solution should be sought from Staffordshire ICT through their Line Manager.

3.4 Protective Marking Scheme

- Staffordshire County Council has implemented this scheme to help protect against data loss. If SCC were to suffer a serious breach then it would damage its reputation with our clients, residents of Staffordshire and our partners

- A protective marking scheme is a way of assigning information to a security level which, in turn, relates to a range of pre-defined controls designed to ensure the information is handled properly.

- On 6 April 2010 the Information Commissioner gained new powers to fine organisations up to a maximum of £500,000 for data security breaches. This scheme is one of the activities we are undertaking to ensure the security of the information that we hold. A list of the most recent fines can be accessed here

- All documents should be securely marked with one of the security levels. Note for "Public" level, the document does not need to be marked. The security levels are:

PUBLIC	No need to mark document
SCC USE	Not for release to the public
RESTRICTED	Not for release to all staff
CONFIDENTIAL	**Would cause serious damage if released**

- As long as the mark is clearly visible, it can appear anywhere – as a standard, marking for emails should appear in the subject field; for other documents in the header or footer.

- It is important to note that just marking documents with an appropriate level is not sufficient to protect against data loss. There are controls in place which govern how the documents can be managed. It is these controls that will help towards maintaining the security of our data.

- It is important to ensure that all information is handled correctly and great care must be taken when sending or transmitting confidential personal data externally.

- The Protective Marking Scheme will help to inform decisions regarding the life cycle of data covering storage, sending and disposal.

- Further guidance on the Protective Marking Scheme can be accessed here. Appendix B shows the comparison between Staffordshire County Council's and the Government Protective Marking Scheme.

3.6 Confidentiality

- Staff must follow their professional codes of conduct and any relevant legislation when handling confidential information.

- Individual staff members are accountable for their own actions, however teams should work together to ensure that high standards of confidentiality are maintained.

- Information obtained through the course of employment should remain confidential to that environment and should not be discussed in a non-work environment. This extends to when your employment or placement has ceased.

- Any breach, or suspected breach, of confidentiality should be reported to the Head of Information Governance.

3.7 Privacy

- Mishandled data can have serious repercussions for organisations, their employees and their customers including; financial penalties, negative press, damage to reputation, customer distress, loss of trust and business and for employees, the possibility of disciplinary action.

- This policy, in conjunction with other SCC policies, outlines what steps to take in order to process personal data in a secure manner and in line with the requirements of the Data Protection Act 1998.

- Staff should be aware that personal data can be visible to other members of staff and visitors when working in open plan offices, therefore staff must take precautions to keep this to a minimum where possible.

- There may be staff that unintentionally access or hear about sensitive personal data that they would not normally have access to as part of their daily job. Any member of staff found in this situation must not disclose this information to anybody else.

3.8 Sharing

There may be circumstances where the Council will need to share personal data. This may be as part of an on-going sharing agreement with another organisation or as a one off disclosure, for example information may be shared with the Police to assist them in the prevention and detection of crime.

The Information Governance Unit can provide advice in ensuring that legislative requirements are being met when data is being shared or transferred to another organisation.

3.9 Social Networking Sites

Staffordshire County Council actively communicates with members of the public through social networking sites like Facebook. The aim of their corporate use is to support the county council in communicating with a variety of groups of people who use this media as their main source of information and are not reachable through

other, more traditional channels. You should ensure you have read the SCC Social Network Policy available on the intranet.

3.10 Bulletin Board

Staff must read and accept the Terms and Conditions of use before using the bulletin board.

3.11 Internet Based Email Accounts

Internet based email accounts include but are not limited to Hotmail, Gmail, Tiscali, and Yahoo. Employees are not permitted to forward County Council information to any internet based email account. If there is a requirement to work from home, Staffordshire ICT can provide access to Outlook Web Access (OWA). This facility enables employees to access their email from any computer with internet access. Staff can have access to wider network resources via Citrix Access Gateway.

3.12 Personal Network Storage

Popular examples of Personal Network Storage are Dropbox and Yousendit Members of staff must not use these external sites for transferring or storing personal data. If staff have a requirement to store, transfer or share information they must obtain advice from Staffordshire ICT and the Information Governance Unit who will be able to offer options to achieve this securely.

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: