Cumberland Council

Information Security Acceptable Use Policy

Version: 2.0
Published: 29 May 2025

Document Control

Related Documents

Title	Author	Version & Date

Revision History

Release Date	Revision Version	Summary of Changes
31/05/2023	V0.1	Initial draft
18/12/2023	V0.2	Final draft
01/04/2024	V1.0	Publication
29/05/2025	V2.0	Review and Publication 2025

Reviewed By

This document (or component parts) has been reviewed by the following:

Post or Group Title	Revision Version	Approval Date
Information Security Officer	V0.1	31/05/2023
Information Security Officer	V0.2	18/12/2023
Information Security Officer	V1.0	04/03/2024
Information Security Officer	V2.0	12/03/2025

Document Approval
This document requires the following approvals:

Post or Group Title	Revision Version	Approval Date
Information Security Manager	V0.1	31/05/2023
Information Security Manager	V0.2	18/12/2023
Information Security Manager	V1.0	04/03/2024
Information Security Manager	V2.0	21/03/2025

Authorised Signatory

Senior Information Risk Officer (SIRO)	V1.0	04/03/2024
Senior Information Risk Officer (SIRO)	V2.0	22/05/2025

Contents

1. Introduction

1.1. Overview

Information and information systems are important assets to the council so it is essential that the council takes all of the necessary steps to ensure that they are at all times protected, available and accurate to support the council's operation and continued success. In addition the council acknowledges that it must demonstrate to its stakeholders its commitment to, and delivery of effective information security.

The aim of the council's Security Policy, Standards and Guidelines is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by the council. These policies, standards, guidelines are used as part of the information security management system (ISMS) within the council.

The council allows all employees' access to appropriate information systems and technology, including the council network, internet and email. This standard sets out the standards applicable for the use of information and information systems within the council.

Some systems require you to acknowledge this Acceptable Use Policy (AUP) before allowing Log On, however, the AUP is applicable to everyone who uses council ICT irrespective of whether specific confirmation is required or not.

1.2. Scope

This policy applies to ALL employees. This includes temporary or contract employees, elected members, volunteers and third parties working for or on behalf of the council. It also includes partner organisations delivering services on behalf of the council and others who have been given access to internal council systems in support of service delivery. These organisations will be further covered by information sharing agreements.

Throughout the document this grouping will be referred to as System Users.

The purpose of this policy is to ensure that all System Users understand their responsibilities for the appropriate use of the council's information technology resources. Understanding what is expected will help System Users to protect themselves, colleagues, the council's reputation, council equipment and information

1.3. Responsibility

Review and Maintenance	Information Security Manager
Approval	Corporate Governance Group
Local adoption	Line Managers
Compliance	All System Users

2. Policy

As the coverage of this is policy is quite wide, it has been divided into several sections, all of which are applicable to all System Users.

2.1. ICT Equipment and the Network

2.1.1 Context

The council has an established and increasingly sophisticated IT infrastructure that underpins all areas of the organisation. This allows System Users access to information in order to allow them to do their jobs effectively.

2.1.2 Business Use

Equipment is provided on the basis of business need. Use of the equipment provide for business purposes is acceptable only where such use falls within the normal day to day remit of the individual.
In particular, the following guidelines must be applied:

- System Users must not deliberately cause any form of damage to the council's ICT systems, or to any of the accommodation of services associated with them.
- System User must not engage in the intentional access, creation, storage or transmission of material likely to bring the council or its services into disrepute.
- System Users must not deliberately undertake activities that would otherwise act against the aims and purposes of the council as specified in its governing documents or in rules, regulations and procedures
- System Users must not deliberately undertake in activities that contravene applicable laws or regulations
- System User must not create, store or transmit material, including software, films, television programmes, music, electronic documents and books that infringe the copyright of another person, except where explicit permission has been given and can be evidenced
- System Users must adhere to the terms and conditions of all licence agreements relating to ICT Systems which they use including software, equipment, services documentation and other goods.
- System Users must not modify any software nor incorporate any part of the provided software into their own work without permission from the designated authority.
- System Users must not load onto the ICT Systems any software. If software is required it must be requested from ICT who have dispensation to do this.
- System Users must not deliberately introduce any virus, worm, trojan horse or other harmful or nuisance program or file into any ICT Systems, nor take deliberate action to circumvent any precautions taken or prescribed by the council to prevent this.
- System Users must not create or transmit material that breaches confidentiality undertakings in a manner which interferes with those activities covered within the definition of Acceptable Use.
- System Users must not use Artificial Intelligence / Intelligent Automation tools without complying with the council's AI Policy
- System Users must not delete or amend the data or data structures of other users without their permission.
- System Users must not in their use of ICT systems exceed the terms of their registration. In particular they must not connect to any other computing ICT systems without the permission of the designated authority.
- System Users of networks and remote ICT systems shall obey any published rules for their use.
- System Users must not attempt to gain deliberate access to information, facilities or services which they are unauthorised to access
- System Users must ensure that they start and terminate each session of use of ICT systems in accordance with published instructions.
- Consumables including stationery must be used for the purpose for which they are supplied and their consumption must be minimised as far as is reasonably possible. Used and scrap paper must be disposed of so as to minimise any risk of a breach of the Data Protection Act 2018.
- System Users must not interfere with the use by others of the ICT systems; they must not remove or interfere with output belonging to another user.

- The creation, display, production or circulation of offensive material in any form or medium is forbidden.
- System Users must take every precaution to avoid damage to equipment caused by smoking, eating or drinking in its vicinity.
- System Users must not engage in excessive internet usage on non-work related matters.
- System Users must not perform actions that could cause any of the council's Information Systems to be overloaded, impaired, disrupted, curtailed or denied (for example watching broadcasts of sports events for prolonged periods).
- System Users must not contribute to News Groups, Chat Rooms or web sites that advocate illegal or undesirable activity or are in contravention of the council's standards.
- System Users must not access, download or transmit any material that is designed to / is likely to offend, harass, insult, bully, threaten, deceive or inconvenience other people, including extremist content and the promotion of related content.
- System Users will not copy any material to any portable device with the intention of unauthorised disclosure
- System Users will not intentionally provide access to equipment or systems for unauthorised persons
- System Users will not use unencrypted USB devices in any circumstance
- System Users will not make use of the wireless connection for purposes other than council business / work, aside from limited personal use as described below
- At times ICT may need to remotely connect to your device to provide assistance via screen takeover. This is permitted under the AUP, however approval must be given by the user to allow them to do this.
- System Users must not remove the SIM card from council issued devices

If in doubt always check with the ICT Service Desk or the Information Security Manager. If you have to think whether it is acceptable, it probably isn't.

The use of personal devices (Bring Your Own Device (BYOD)) for council business is prohibited unless prior authorisation has been given by the Information Security Team for exceptional circumstances.

Equipment and systems are provided to System Users for business purposes, however the council wishes to encourage System Users to develop their IT skills and acknowledges that formal training is often best complemented by "trying things out" or personal use.

Personal use, however, represents an area of concern not just in the council, but in all sectors given the risks faced.

It is the council's view that limited personal use is acceptable but this must be confined to non-business hours and must, at all times, be legal. Further, such use must only be for personal purposes. The use of council equipment to support or pursue private businesses is not acceptable. Some examples of acceptable personal use could include such things as a personal letter to your bank, maintaining or updating your CV or completing college assignments.

Some examples of unacceptable use could include the storage of illicit, pornographic or racist material or the use of the equipment to duplicate copyrighted materials such as software or music. This is not an exhaustive list.

System Users must not install personal software on council equipment regardless of its nature. Only software which supports council business is to be installed and in all instances this must only be done if approved by the ICT department following an ICT Service Desk request.

In all instances, usage can only be acceptable if it is by a council employee / contractor. Use of equipment by family or friends is unacceptable regardless of the purpose of use.

2.1.3 International Use

Council ICT equipment (including but not limited to laptops, mobile phones, tablets, SIM cards, 2-factor authentication dongles and encrypted USB sticks) must **not** be taken outside the United Kingdom. Exceptions to this policy may be granted by the Senior Information Risk Owner (SIRO) in exceptional circumstances.

Due to the severity of the cyber threat, it is unlikely that a System User's request will be granted by the SIRO but a request will be considered based upon exceptional business requirement. A risk assessment will be undertaken on a case-by-case basis taking into account essential business needs, the country of desired destination and the latest security and threat intelligence available. If the request is granted additional security controls must be adhered to.

System Users must submit a request via the ICT service desk at least 14 days prior to travel. If approval is granted, the System User must provide written confirmation that they will adhere to additional security controls. System Users can email security@cumberland.gov.uk to discuss matters prior to submitting a request.

It is important to note that all council equipment is encrypted to protect council data and configuration. An increasing number of countries have made the possession of encrypted electronic devices illegal or have prohibited specific technology such as VPN connections. Use of equipment abroad may also be subject to prior licencing /visa approval before being taken into a county. This has increased the risk of travellers being detained by security authorities. This may be beyond a traveller's control if a place is diverted in an emergency for example.

System Users must not remove the SIM card from a council issued device such as a mobile phone and must not insert the SIM card into a personal device to take it abroad. This is prohibited.

2.1.4 Upon Leaving the Council

Upon leaving the council, it is the responsibility of the System User to ensure that all council equipment is returned to the ICT department before or on the last day of the System User's employment. The System User must obtain a receipt and retain this for their records.

If the System User does not do this, the System User accepts that they will be invoiced for the value of the equipment and associated recovery costs.

2.2. Personal Details

System Users will be given an active directory account which will enable them to log in to the council network. This account will hold their work details such as job title, office location and telephone numbers. Periodically they will be prompted to update these details via a pop-up window when they log in. System Users must ensure that these details are correctly completed. Where the details include a photograph this must be a true likeness appropriate for business use; a head and shoulders image is the most appropriate.

2.3. Email

2.3.1 Context

Email is an essential business tool, facilitating the sharing and dissemination of information between staff and beyond organisational boundaries. While essential to the effective operation of the council there are risks to its use as has been demonstrated in highly publicised cases in the media.

Emails sent over the internet are not secure unless further controls have been applied. Unless the email is encrypted, both incoming and outgoing emails can be intercepted using commonly available tools. The council currently uses Egress to encrypt emails. Most staff have access to an encryption tool to send council information to an external email address. System Users without access to the encryption tool may email security@cumberland.gov.uk to discuss solutions. Emails sent internally can be treated as secure as they do not pass outside the council's systems.

Under no circumstances must sensitive or Personal Identifiable Information (PII) be transmitted by non-secure email unless it is encrypted. Sending / auto-forwarding any council data to a System User's personal email account is prohibited.

The content of all email stored on equipment owned by the council remains the property of the council. System Users must **not** have an expectation of privacy in anything they create, store, send or receive on their computer.

The council has the capability and right to monitor emails if there are suspicions of inappropriate use. In addition the council monitors unencrypted external emails for sensitive or personal data. Should a user leave the council, access to the emails will be granted to the System User's manager or appropriate System Users as requested by the System User's line manager.

2.3.2 Business Use of Email System

The council's email system is, essentially, a business facility. System Users must be aware that email is legally attributable to the council in exactly the same way as letters/fax/memos and therefore information, which could be construed as legally binding, must not be transmitted over email.

A disclaimer is automatically added by the council's email system to every outgoing email as follows:

This email contains confidential information (which may also be legally privileged) and is intended solely for the use of the intended named recipient.
If you are not the intended recipient you may not disclose, copy, distribute or retain any part of this message or its attachments. If you have received this message in error please notify the originator immediately by using the reply facility in your email software. Incoming and outgoing emails may be monitored in line with current legislation.
All copies of the message received in error must be destroyed.
Any views or opinions expressed are solely those of the original author. This email message has been scanned for viruses, and declared to be virus free at the point of exit from the council's network.

This message is not added to emails sent between internal council mailboxes.

The council email system allows System Users to retain in their mailbox of email and attachments. System Users are responsible for managing their own mailboxes and ensuring that messages which are no longer required are deleted. System Users must be aware that sending large attachments affects the performance of the network and therefore attachments should not be sent by email where the total size of the email including attachments would exceed 150Mb which is the maximum limit allowed via Microsoft office 365.

To aid System Users, a number of key do's and don'ts are set out below:

DO	DON'T
✓ Think carefully when composing mail, the nature of email is that it is often less formal than letters etc. This informality can cause differences in interpretation amongst recipients. ✓ Use distribution lists appropriately. Is it important that all addressees receive this email? ✓ Check your emails regularly, and respond to requests promptly. ✓ Advise people when you are not available by setting 'Out of office auto-reply' on the system. ✓ Be selective about who receives your emails, especially when using 'Reply to All'. Do all recipients need to see the reply? ✓ Use BCC not CC if you do not have permission to disclose the addressees' email addresses. ✓ Review the email trail and delete if not required or appropriate. ✓ Remember that a mail from a council email account reflects on the organisation. It is also admissible in a court of law and may require disclosure under the Freedom of Information Act. ✓ Manage your mailbox. ✓ Keep your password secure. ✓ **Ask if you are in doubt.**	❖ Send personal identifiable information by email without the Information Security Manager or Department Manager's approval. ❖ Make commitments via email or the Internet on behalf of the council without full authority. ❖ Send offensive, pornographic or illegal messages or material. ❖ Use the email accounts of others except where permissions have been granted by the ICT Service Desk. ❖ Send global messages, except for alerts ❖ Send messages to those whom you are aware do not wish to receive the mail. ❖ Use the account of another individual without official access to that account. ❖ Use the email system for personal gain. ❖ Forward junk mail, spam or chain mail. ❖ Send emails larger than 35Mb including attachments. ❖ Open mail where you do not recognise the sender or the contents appears to be dubious – it may be a virus. ❖ Falsify emails so they appear to have originated from someone else. ❖ Open attachments with exe or vbs extensions. ❖ Be caught out by the speed of email. Think carefully, is your first reaction really the one that you want the recipient to receive.

2.3.3 Internet Mail

Messages sent using commercial internet mail accounts (such as Yahoo, Gmail or Hotmail) are particularly insecure and staff must not to use them for council business. Many of these services are operated outside the European Union which potentially impacts on the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

2.3.4 Personal Use of Email

The council email service is provided to System Users for business purposes, however the council wishes to encourage System Users to develop their IT skills and acknowledges that formal training is often best complemented by "trying things out" or personal use. Personal use, however, represents an area of concern not just in the council but in all sectors given the risks faced.
It is the council's view that limited personal use is acceptable, but such usage must not interfere with the performance of your job, therefore use of email facilities for personal purposes must be confined to non-working hours.

Further, such use must only be for personal purposes and must not be to support or pursue private businesses. System Users must be particularly careful regarding the content of emails; for example, jokes or images may be unacceptable.

In particular, System Users must ensure that:

- Personal use is kept to a level that is not detrimental to the main purposes for which the accounts were provided
- Priority is given to the use of accounts for business purposes
- Personal use must not be for commercial purposes or any form of personal financial gain
- Personal use must not conflict with council policies and procedures
- Personal use must not conflict with any of the System Users obligations as a council employee

2.4. Messaging

Text Messaging is generally an insecure method of information transfer. No sensitive information may be sent via text. As messages are so short, great care needs to be taken to ensure that business related texts sent convey the message intended by the sender, are not ambiguous, and can't be misconstrued.

The risks surrounding the use of WhatsApp messages for work purposes should also be considered by System Users. WhatsApp messages can be legally disclosable e.g. as part of a Subject Access Request (SAR), Freedom of Information Request (FOI) or under data protection rules. They may also be used during workplace conduct reviews. Where required by the service, all WhatsApp messages are to be uploaded into the appropriate corporate application and retained.

2.5. Video Messaging

Video Messaging can be provided by a number of applications such as MS Teams. These are communication tools that allow real-time desktop video conferencing and Instant Messaging. No sensitive information may be sent by Instant Message and caution must be exercised in using the video facilities to communicate confidential or sensitive matters. The facilities must not be used in public spaces where the conversation may be overheard.

2.6. Voice or video recording

It is sometimes easier to make a voice recording of meetings and use the recording to document the meeting at a later date, whether as 1:1, group meetings or telephone calls. The Data Protection Act 2018 and Regulation of Investigatory Powers Act 2000 both cover this area and need to be taken into account.
Prior to recording any conversation or meeting:

- Notify the attendants of your intentions.
- Notify the attendants the purpose for which the recording will be used.
- Notify the attendants of how long the recording will be retained before disposal.
- Get approval from the attendants that this is acceptable.
- Where approval is not gained in advance the recording cannot be used and must be destroyed immediately.
- Permission to use the recording may not be granted retrospectively.
- Ensure that the recording is stored on media which is encrypted to a standard accepted by the council. For more information please speak to the Information Security Manager.

2.7. The Internet

2.7.1 Context

The internet is a valuable tool for research and dissemination of information. However, the risk associated with connection to and use of the internet is extreme and requires significant management and control.

2.7.2 Business Use

Internet access is seen as a key facility in enabling System Users to perform their jobs. Access to web sites and services which are to support business (e.g. research) activities are deemed to be acceptable.

Filters are in place to prevent council resources being used to access extremist content or to promote related materials on the council's network. If a System User notices the ability to access inappropriate sites and content (which are not blocked by council systems) then System Users must report their findings to security@cumberland.gov.uk immediately.

2.7.3 Personal Use

Internet access is provided to System Users for business purposes, however the council wishes to encourage System Users to develop their IT skills and acknowledges that formal training is often best complemented by "trying things out" or personal use.

It is the council's view that limited personal use is acceptable but such usage must not interfere with the performance of your job, therefore use of the internet for personal purposes must be confined to non-working hours.

At all times there are a range of conditions that must be applied to such access via:

- System Users must not access, download or transmit any obscene, indecent or pornographic images, data or other material
- System Users must not access, download or transmit any defamatory, sexist, racist or otherwise offensive images, data or other material
- System Users must not access, download or transmit any copyrighted material in a manner that violates that copyright, breaches licence agreements or data privacy rules, including but not limited to piracy or illegal streaming.
- System Users must not access, download or transmit any material that is designed or likely to annoy, offend, harass, insult, bully, threaten, deceive or inconvenience other people, including extremist content and the promotion of related content
- System Users must not access, download or transmit material created for the purpose of corrupting or destroying the data of other users
- System Users must not allow non-council persons access to systems
- Use must be for personal purposes and not for the support of any private business ventures
- System Users must not use council processing power for anything other than its intended use (i.e. Crypto mining).
- System Users must not use Artificial Intelligence / Intelligent Automation tools without complying to the council's AI Policy.

Such guidance does not represent the totality of possible inappropriate access. System Users must be aware at all times that the principles of decency and legality will be applied. A simple rule of thumb could be described as "if the material could cause offence to even one individual then it is probably inappropriate"

The final "decision" on the appropriateness of material accessed will lie with the council. It is the council's view that limited personal use is acceptable but this must be confined to non-business hours and must, at all times, be legal. Further, such use must only be for personal purposes. The use of council equipment to support or pursue private businesses is not acceptable.

Filters are in place to prevent council resources being used to access extremist content or to promote related materials on the council's network. If a System User notices the ability to access inappropriate sites and content (which are not blocked by council systems) then System Users must report their findings to security@cumberland.gov.uk immediately.

2.8. Cloud Services

The National Cyber Security Centre (NCSC) has detailed security principles that should be considered when implementing a cloud solution. In order to ensure that these have all been adequately considered, any use of cloud

services or storage may only be implemented after consideration and approval in advance by the ICT Department and the Information Security Team. Any proposed contracts with third party suppliers will also have to be considered by Legal Services. No cloud service may be used or contracts entered into without this prior approval.

2.9. Mobile Equipment Protection

Laptops, tablets and mobile phones are valuable pieces of equipment in themselves, regardless of the information stored on them. Consequently, care must be taken to look after the equipment and protect it from damage or theft. For reference:

- Use your council managed and supplied equipment for agile working. Use of any unmanaged equipment must be risk assessed before used for remote working
- When not in use, ensure your equipment is safe. If the equipment is left in the office overnight or at weekends, it must be put out of sight of potential intruders (such as in a desk drawer).
- Keep your equipment with you in its case when you are travelling. Vehicles are not safe place for expensive equipment even if out of sight (although it is recognised that in certain circumstances this may be unavoidable). If you do need to leave the equipment in an unattended vehicle, it must be placed out of sight in the boot at the point of departure. It must never be placed in the boot at the point of arrival where such action may be observed when the vehicle is being left.
- Avoid dropping your equipment, even when in its bag. The bags are only capable of withstanding a small amount of shock.

2.10. Data Protection

System Users can be personally prosecuted for unlawful activities concerning misuse of personal data. System Users must make sure they have proper authorisation for everything they do with personal data. They must ask their manager and/or directorate Data Protection Co-ordinator for guidance if unsure about collecting, transferring, sharing, disclosing, editing, storing and deleting personal data.

System Users may be given access to confidential or personal data as part of their job role. Such access is only to be used for matters relating to their job as permitted by their departmental policy. Access for reasons outside this is strictly forbidden. Moreover, if a System User is asked to access the data of a service user who is known to them personally then specific written approval is to be obtained from their line manager before doing so. Access to such data for personal reasons is strictly forbidden.

Should a System User leave the council, access to the System User's data held in locations such as OneDrive, "My Documents", or within shared document areas where the System User is the owner / administrator (e.g. SharePoint) will be granted to the System User's line manager.

Further notes:

- Any personal information held can be asked for by the data subject concerned (e.g. a member of the public) as a subject access request. This means all System Users must ensure that any comments or opinions about living individuals are acceptable to share with the same.
- Data within the council must be handled in accordance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). Particular care is required for Personal Identifiable Information (PII).
- PII must never be stored locally on the device unless there is no other alternative and must be agreed with the line manager (after consulting the Information Security Manager if necessary) prior to storage. Local storage will only be acceptable if the device is fully encrypted or on the hard drive of a pc situated within council premises.
- If PII or sensitive data needs to be accessed via the device, the data needs to be stored on secure server which the device is linked to, even when using desktop PC's. As well as the security risks, data stored locally is at risk from hardware failure and data loss.
- PII or sensitive data can be sent within the council but must **NEVER** be sent to external employee personal email accounts such as xyz@hotmail.com unless specifically authorised by the Information

Security Manager and may only exceptionally be sent to non-council accounts (e.g. Audit Commission) when Secure File Transfer is not feasible.

- As part of the preparation process the sender must get written/electronic agreement from the recipient that they will use the data as intended and dispose of the data as agreed with the sender and/or the Information Security Manager.
- The sender must ensure that the tracking options are enabled on the email, this will ensure that the sender receives a received receipt when the email arrives in the recipient's inbox and a read receipt when the email is opened and read.
- The password / key MUST NOT be transmitted in the same email but must be either sent separately to the named recipient or telephoned through to them. The sender must speak to the recipient and not leave a message for them with someone else or leave a message on an answer machine. Note: For regular transfers of information as part of a sharing agreement it is possible to set a password in advance and use this for all secure email correspondence with them.
- Should password or keys be lost by either end there is a possibility that the data transferred might not be decrypted and could be permanently lost. To avoid this the sender needs to save a copy of the data on a secure network server in case of loss.
- No PII or sensitive data shall be stored on removable media unless a risk assessment has taken place and it is determined that it is necessary for the data to be stored on this device. If at all possible, an alternative method shall be sought.
- If PII or sensitive data is to be stored on removable media this data must be encrypted to 256 bit AES. Encrypted USB removable media are available from the Corporate Procurement Catalogue.

No PII or sensitive information may be shared with partner agencies and third parties unless a Data Protection Impact Assessment (DPIA) has been carried out and an appropriate information sharing agreement and protocol is in place. These must be approved by Information Governance before any data sharing takes place.

Where possible email must be avoided for transferring PII internally. In preference suitably protected data directories or SharePoint libraries must be used. These can be arranged through the ICT Service Desk.

2.10.1 Personal equipment

As the council has no control over and cannot ensure the security of your personal equipment (e.g. personal computer, laptop, tablet, mobile phone, etc), System Users are not to transmit to or from, process, copy or store PII or sensitive data on personal equipment. Such data must **NOT** be emailed to System Users' personal email accounts.

2.10.2 Printing

Care must be taken when printing council information, especially when it contains PII. Printed material must not be retained for longer than required and must only be kept away from council premises if immediately required. Under no circumstances may printed material containing PII be stored in non-secure locations (e.g. at home). All printed material containing PII must be securely destroyed. Agile or Remote workers are to refer to the Agile or Remote Working Policy and should ensure that secure storage is used.

2.10.3 Logging

System logging and monitoring exists throughout the council's corporate network. This is required to protect individuals, to comply with legislation and for investigative purposes. In most cases logging will be stored for a maximum of 6 months and will be made available to line managers, HR and external agencies such as the Police for investigation purposes. Examples of the type of information which will be logged (not exhaustive):

- Username
- Name of person
- Department of person
- Source device
- Destination device, service or URL
- Date and time of access

- Status of access (Permit, Denied or Rejected)

If you are conducting an investigation and require access to this type of information please speak to the Information Security Manager or the ICT Service Desk about your requirements. However, please be aware that some of this information can take time to recover. In some circumstances, this information may be released due to a request under the Freedom of Information Act. In these circumstances personal information will not be disclosed.

2.10.4 Tracking, configuration and Location Data

The council may use technology to track the details of hardware, software and data for the purpose of providing configuration management, auditing and crime prevention. This technology may be used to track devices and may be provided to third parties such as the police for further investigation. The council will endeavour to enable this technology on all supported devices at all times. Unauthorised System Users must not attempt to disable override or modify the protection.

2.10.5 USB Devices

USB ports are disabled by default and all USB devices are controlled through software and need to be authorised in order to work. The number of security risks related to USB devices has increased dramatically over the past few years and the ICT Service has implemented this software to reduce risk. Certain devices provided by the ICT Service such as Hardware Encrypted USB devices have been automatically approved, however if you have devices such as cameras or specialised input equipment you will need to discuss the requirements with the ICT Service to ascertain whether they can be approved.

In addition you are **not** permitted to connect any peripheral equipment which has not been supplied by the council or specifically authorised by the Information Security team. This includes any item for which you are not intending to access data and for which you only require the USB port for power either to operate or to recharge, such as fans, lamps, Bluetooth speakers, electronic cigarettes, smart watches, personal phones, Christmas lights etc.

2.10.6 Leaving a computer unattended

In order to prevent unauthorised access when a computer is left unattended, System Users are to lock their computers if leaving them for a short period (e.g. using the key combination of Windows Key + L or Control, Alt, Delete then selecting “Lock this computer” or via the Start button). In addition the council has in place a setting which will lock the computer automatically after a certain period of inactivity. There may be circumstances (e.g. when giving a presentation) when this is inappropriate. A temporary lifting of this restriction can be requested through the ICT Service Desk.

2.10.7 Passwords

Access to the council’s Information Systems and to various applications is protected by users’ passwords. These passwords should be complex. The council currently requires them to be a minimum of 12 characters in length and they must be a combination of upper case and lower case characters, numbers and symbols. It is recommended that they are based on a minimum of 3 random words. Guidance on how to formulate passwords will be provided from time to time and as part of the annual security training. Some System Users will be required to change their passwords periodically; currently every 56 days. System Users must not share their passwords or write them down, however System Users must divulge their password to the Information Security Manager if instructed to do so as part of any investigation. If a System User has more than one council account then each account must have a unique password.

2.10.8 Security Key Fob (Agile and Remote Access users only)

In order to remain compliant with external audits and to reduce our external security risks, we have introduced security key fobs which generate a unique one time password each time you login when you are away from the office. The security key fob can be a physical token or a software token on your work or personal smartphone but it is important that you protect your token in the following ways:

- Your 4 digit pin code must not be written down and must never be stored together with your fob.

- Any loss, damage, theft of your security fob must be reported to the ICT Service Desk as soon as possible.
- If you leave the authority or no longer require remote access, return the security key fob back to the ICT Service Desk so that it can be re-issued or disabled.
- Delete the smartphone application from your personal smartphone if no longer required.

2.10.9 Clear Desk Policy

The council's agreed principle is to implement a clear desk policy. All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet when not in use.

Confidential waste shall be disposed of in the confidential waste bins within council offices.

3. Agile or Remote Working

System Users must comply with the Agile or Remote Working Policy and the full suite of Security Policies.

If an issue arises while working away from the office then the System User must immediately report to security@cumberland.gov.uk and their line manager.

Agile or remote working includes working in environments such as third party offices, public spaces (e.g. council libraries) and at home. Use of council equipment outside the office is permitted but the System User is responsible for working in a secure manner.

System Users must only connect to trusted Wi-Fi sources e.g. council libraries but these may only be used to establish a VPN connection with the council network. Direct access to council systems or any external resources such as the internet is not permitted; all access must be made using the VPN connection

Examples of unsecure Wi-Fi sources include coffee shops, shopping centres and hotels. If you have to use an unsecure Wi-Fi network in exceptional circumstances, VPN **must** be used.

System Users should be particularly vigilant to ensure that they are not overlooked by other people or by equipment such as CCTV and that any confidential data displayed cannot be read by unauthorised persons. This not only includes the screen but also any paperwork.

Confidential information should never be discussed in a public place. System Users should also take care that they cannot be overheard when discussing any work matters with colleagues and when using voice services such as MS Teams and mobile phones. As well as being overheard by people in the vicinity, System Users must be mindful of any equipment which can record audio, especially if it is connected to the internet. Examples of such equipment are smart TVs and other connected devices like Amazon Echo (Alexa), Google Home (Google Assistant), Siri enabled devices (Apple), Ring Door Bells etc.

System Users should be cautious about taking out any paperwork and should ensure that nothing is left behind when they leave.

If in any doubt about the security of the public environment users should not undertake any work-related matters; there is no criticism in erring on the side of caution.

Mobile communication devices must **not** be taken outside the United Kingdom. Exceptions for over-riding business reasons may be authorised by the Senior Information Risk Officer (SIRO) on a case-by-case basis and written authority must be obtained in advance.

4. Protocol for Other Uses

Where Information Systems are to be used for purposes other than acceptable use as defined by this policy, that use must be authorised in advance by the Information Security Manager via the System User's Line Manager.

4.1. Privileged Accounts (System Administrators only)

In order to manage the ICT Service, the council is required to provide some System Users with privileged accounts which are used to perform actions required for their job role. Any action completed using a privileged account must be authorised and must be completed in compliance with the Change Management Policy. Any unauthorised use may be subject to the council's disciplinary procedures.

In some scenarios, System Users will be provided with three accounts; one standard account used for normal day to day activities, one management account used for logging on to servers and one admin account used for performing administrative tasks. With reference to these accounts, the following requirements must be obeyed at all times:

- Login credentials must be unique (per account) and must not be shared.
- Account passwords must not be the same as those used for other accounts.
- Account passwords must be formulated and changed in line with the council's password policy
- Admin accounts must not be used to log on to servers and must be used with the "Run As" feature in order to perform privileged actions.
- Management and Admin accounts must not be used for remote access capabilities.

Local administrator passwords will be available to a limited number of system administrators. This type of account will only be used in situations where a device is unable to connect to the domain or all other logins fail. Other circumstances which require the use of the local administrator password must be approved by the Information Security Manager or a member of the ICT senior management team.

5. Training

All System Users must undertake Information Security training in order to be given or to retain access to the council's Information Systems. This training is to be undertaken when first given access, at least annually thereafter and on any other occasion as required by the council. The method of training will be determined from time to time by the council. System Users will be notified when such training is required and failure to undertake this training may result in the System User's access privileges being withdrawn.

6. Reporting / Queries / Feedback

All suspected or actual incidents (such as loss of assets, tampering, compromise of information) must be immediately reported to the System User's line manager, security@cumberland.gov.uk and the ICT Service Desk.

Any queries which a System User has should also be directed to the ICT Service Desk in the first instance.

7. Applicable Regulatory Framework

System Users are bound by the Law of England and Wales when using the council's Information Systems. In addition, when accessing computers abroad, the laws of that country apply. It is the System User's responsibility to ensure his or her activities comply with these laws. The council Information Security Manager can assist in the provision of guidance to relevant domestic legislation.

The use of the council's Information Systems is subject to all relevant council regulations.

When making use of the Internet, the acceptable use policies of the Internet Service Providers apply in addition to this policy.

8. Prevention of Misuse

The council retains a right of access to all information held on its Information Systems for the purposes of investigating misuse including information held in folders that individuals have marked 'personal' or 'private'.

Monitoring may take place periodically within the guidelines set down by the Regulation of Investigatory Powers Act 2000 ('RIPA'). The council retains the right under RIPA to access all information held on its Information Systems to monitor or intercept any system logs, web pages, email messages, network account or any other data on any computer system owned or operated by the council. This will be for the purpose of preventing, detecting or investigating crime or misuse, ascertaining compliance with regulatory standards and council policies, or to ensure effective system operation.

In order to guard against abuse of the Information Systems, Internet use is constantly monitored, email is scanned for profanity and other inappropriate content and the use of corporate telephony may be subject to monitoring at any time, particularly when there is reason to believe that misuse is occurring. Telephone conversations will not be subject to interception.

The council's policy on the prevention of misuse is:

- to make all employees, temporary or contract employees, elected members and third parties working for the council, as well as partner organisations delivering services on behalf of the council and others who have been given access to internal council systems aware of this Acceptable Use Policy
- to educate employees, temporary or contract employees, elected members and third parties working for the council, as well as partner organisations delivering services on behalf of the council and others who have been given access to internal council systems in matters relating to acceptable use
- to take swift and effective action within existing disciplinary and/or legislative frameworks against anyone found to be misusing the council's Information Systems.

9. Disciplinary Procedures

Where misuse of the council's Information Systems has been identified, the matter will be the subject of investigation in accordance with the appropriate disciplinary procedure and/or legislative framework. Investigations will be carried out by the Information Security Manager or an appropriate designated officer.

10. Libel

Libel is a civil wrong, which in proven cases may incur substantial compensation. It is very complicated and therefore one of the easiest laws to contravene through ignorance. Facts concerning individuals or organisations must be accurate and verifiable, and views or opinions must not portray their subjects in any way that could damage their reputation. Check with the council Legal Department before publicly displaying any contentious material. Web pages, email messages and messages posted on discussion forums are regarded as published material. Refer to the council's **Social Media Policy** for more information regarding the use of this emerging technology.

11. Summary

Be sensible when using council ICT resources:

- The resources are for you to do council work
- Always protect the resources. This will aid in the prevention of unacceptable use
- If the use would cause problems, upset, offence or embarrassment, it is probably not acceptable.
- If you're not sure if something is acceptable, ask for help first.
- Context is important. Security risks increase when working outside your normal workplace.

- Be aware that your use of resources is monitored. During an investigation into a security incident, ICT can capture evidence.
- Above all, if you think there is a problem, ask for help.

The way you use ICT is important because it indicates your approach to work and can be taken into account when assessing your behaviour and performance.