Somerset Council

ACCESS CONTROL POLICY

Access to systems and resources

Document Owner: [Service Management]

Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	15/08/2022	A. Ware	Document first created
1.0	22/08/2022	R. Rooks	Final Version for Technology Gateway
1.1	12/01/2023	R. Rooks	SC Branding Applied
1.2	24/02/2023	R. Rooks	Apply updates from LGR HR & Unions review
1.4	15/03/2023	R. Rooks	Official SC Branding & Executive Member Approval

Document Contents Page

Purpose

The purpose of the policy is to ensure the correct access to the correct information and resources by the correct people.

Scope

People

All employees whether permanent, temporary, agency or contractor and all third parties.

Systems

All systems and applications provided and/or given access to by the council are deemed in scope.

Physical Access

Physical access is defined in the Physical and Environmental Policy.

Access Control Policy

Principle

Access control is granted on the principle of least privilege. Users are only provided access to the information they require to perform their tasks and role.

Confidentiality Agreements

All employees and contractors should sign a user confidentiality agreement prior to being given access to information processing facilities

Role Based Access

Access to systems is based on role. Access is granted by the business owner, system owner or data owner and designated approval processes.

Unique Identifier

Users are assigned a unique username or identifier on the principle of one user one ID to ensure individual accountability. Usernames and identifiers are not shared between users.

Access Authentication

Users are positively identified and authenticated before gaining access to systems, services, or information.

Access Rights Review

User access to systems is reviewed at least annually to ensure it is still appropriate and relevant.

Inactive and dormant accounts are investigated, and appropriate action taken including the updating of required documentation.

The main user access system is reviewed every 90 days to ensure it is still appropriate and relevant.

Privilege Accounts / Administrator Accounts

Administrator accounts are not provided to users, including but not limited to council owned laptops and mobile technology.

Administrator users are assigned specific administrator accounts in addition to their normal account for the specific use on the completion of administrator tasks.

Administrator accounts are not shared accounts, not generic accounts and do not share passwords.

Administrator accounts are clearly identifiable.

Privilege may be granted by the appropriate use of temporary privilege elevation (i.e. MS Privileged Identity Management or Admin by Request) or via a separate account as per administrators as deemed appropriate.

Appropriate privilege and/or accounts will be assessed, authorised and a register maintained by ICT Security Operations.

Privilege and administrator accounts are logged and monitored.

Privilege and administrator accounts are provided for a set period of time.

Passwords

Password usage should comply with the current **ICT 02A Password Policy**

Access to systems and information should always be authenticated by passwords as a minimum

Most systems should be supplemented by a more secure authentication system such as Multi-Factor Authentication, Password-Less, FIDO2, SmartCard or Windows Hello for Business.

Even if not mandated the supplemental options should always be used if available.

This is a recommendation for accessing any service not just in the work place.

Initial passwords provided to users must be changed on first use.

Vendor supplied and default usernames and passwords are changed immediately upon installation or first use. This should include any provided directly to users by third parties and for personal equipment that are used for council business.

NOTE: For everyone’s benefit, the council recommends this approach for all personal non-council devices and access, even if not used for council business and would even extend to home broadband services.

User passwords are not generic, shared or set at a group level.

Passwords are to be kept confidential and not written down.

Passwords are not displayed when entered.

Passwords are not coded or included in any scripts or code or macros.

Passwords are encrypted when transmitted over networks.

User Account Provisioning

Account creation, modification and deletion is performed by authorised personnel and is fully documented.

Individual line managers approve account creation, modification, and deletion.

Business, system, or information owners approve access to systems and information. Processes are used to clearly indicate the required access and suitable authorisation is provided.

Where users are not using the provided self-service mechanisms to reset or change authentication credentials then their identity should be verified by the application owner and/or administrator.

Leavers

Line managers and HR inform the account provisioning team a user's leave date.

When a user leaves the council, all access is revoked, as a minimum to the main authentication technology, and to all systems and data recorded in the role-based access list.

User IDs, passwords and authentication credentials of leavers should be properly reset in case of reuse by ICT as part of the leavers process.

Authentication

The main access authentication system

- Does not display system or application identifiers until the log-on process has been successfully completed
- Display a general notice warning that the computer should only be accessed by authorised users.
- Not provide help messages during the log-on procedure that would aid an unauthorized user
- Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect
- Protect against brute force log-on attempts
- Log unsuccessful and successful attempts
- Raise a security event if a potential attempted or successful breach of log-on controls is detected
- Not display a password being entered
- Not transmit passwords in clear text over a network
- Terminate inactive sessions after a defined period of inactivity, especially in high-risk locations such as public or external areas outside the organization's security management or on mobile devices
- Restrict connection times to provide additional security for high-risk applications

Third Party Remote Access

Access is only granted to third parties under current contract with an applicable non-disclosure agreement and/or Memorandum of Understanding (MoU) in place.

Access is granted for a specific time, to a specific system, to a specific individual and provided by specific agreement including receipt of a formal, valid, authorised access request.

Access is removed immediately on completion of the requirement.

A list of third parties and individuals with access is maintained.

Monitoring and Reporting

Access to systems is monitored and reported and actions that directly or indirectly affect or could affect the confidentiality, integrity or availability of data are managed via the Incident Management process.

Policy Compliance

Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement process. It should be updated and reviewed when necessary but no later than 12 months. This process is the responsibility of the document owner.

Somerset Council

PASSWORD POLICY

Corporate Password Policy

Document Owner: [Service Management]

Document Version Control

	Last Modified	Last Modified By	Document Changes
1.0	09/03/2022	D. Mitchell	Document moved over to new format
1.1	31/08/2022	A. Ware	Rebranded
1.2	01/09/2022	R. Rooks	Align with ISO27001 templates and existing LGR policies
1.3	12/03/2023	R. Rooks	SC Branding Applied
1.4	24/02/2023	R. Rooks	Apply updates from LGR HR & Unions review
1.5	15/03/2023	R. Rooks	Official SC Branding & Executive Member Approval

Document Contents Page

Purpose

The purpose of the policy is to ensure the correct use of passwords in line with current best practice and NCSC recommendations.

Scope

All council employees and external third-party users.

All software, hardware, and virtual services used by employees and external third parties to access corporate services and/or data.

Overview

Cybercrime is now a massive 24x7 threat with an increased risk to our users and their data both at work and at home. The Council needs to adopt a more stringent authentication policy to reduce this threat. The Council also suggests users adopt similar approaches for personal access and can provide guidance as necessary. The policy required for corporate access follows.

Implementation

As far as possible existing systems, applications and devices will comply with this policy and be adapted as necessary. The current aim would be to actually eliminate passwords by using Microsoft Password-less sign-in and/or Windows Hello for Business (WHfB) or equivalent. Improving both the user experience but also their security stance to the mutual benefit of both themselves, the Council and other users.

Where direct password entry remains this will be supplemented when possible with Multi Factor Authentication (MFA) or equivalent.

Where MFA is available, then ideally the strongest forms should be used such as the Microsoft Authenticator application with number matching. Phone calls and SMS texts in the absence of no additional security or more secure options are an advance, but now in turn in the current day offer relatively weak protection.

The Council in future will seek to procure only systems, applications and devices that comply with this policy, using technologies as mentioned above. Password only systems without the ability to use strong authentication should no longer be considered.

Password Policy

Passwords where required **MUST** be created using the following guidelines:

- They must be a minimum of 8 characters long.
- They must contain at least three out of the following four categories: Upper case characters, Lower case characters, Numbers, Symbols (@ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < >)
- Expiration is currently 60 days. This will be increased depending on the resulting strength of authentication security and the sensitivity of a particular application.
- Memorable passphrases of 3 or more random words are strongly recommended. Ideally separated by special characters or numbers (NCSC Guidance) and preferably more than the required minimum of 8 characters.
- Never write down passwords – Use Password Self Service to easily replace forgotten passwords.
- Never disclose or share passwords with anyone including other Council colleagues or team members.

Note: A new password reset/change may fail for less obvious complexity reasons because it may be fully analysed before it is allowed. This involves comparing it with lower case versions as well as substituting numbers and symbols for their commonly used equivalent characters. Obvious repetitions within passwords or similarities with previous passwords will likely be disallowed. Passwords will also be checked for simplicity against regularly updated non-public lists of weak and hacked passwords. The Council will supplement these checks with a custom list of obvious words such as **Somerset**.

ICT will advise as required on best practice approach including non-standard use cases and recommended complexity for retained password only applications.

Policy Compliance

Compliance Measurement

The Information Security Management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement process. It should be updated and reviewed when necessary but no later than 12 months. This process is the responsibility of the document owner.

Somerset Council

ASSET MANAGEMENT POLICY

Assets and configuration

Document Owner: [Service Management]

Document Version Control

	Last Modified	Last Modified By	Document Changes
1.0	06/09/2022	A. Ware	Document first created
1.1	29/09/2022	R. Rooks	Final Version for Technology Gateway Panel
1.2	12/01/2023	R. Rooks	SC Branding Applied
1.3	24/02/2023	R. Rooks	Apply updates from LGR HR & Unions review
1.4	15/03/2023	R. Rooks	Official SC Branding & Executive Member Approval

Document Contents Page

Purpose

The purpose of this policy is the identification and management of assets.

Scope

All council employees and external third-party users.

All council information and physical assets.

Asset Management Policy

Principle

Council assets are known, identified, and managed with appropriate protection in place.

Inventory of Asset

Information and information processing, storing, and transmitting devices are identified and an inventory of these assets is drawn up and maintained.

For each asset, **at least** the following, is recorded:

- The asset name.
- The asset owner
- The importance of the asset
- The classification of the asset

For physical assets additionally, **at least** the following is recorded:

- Asset number
- Serial number
- Whether in use
- Last checked by and date
- What the asset does
- A description of the information process, stored or transmitted

Ownership of Assets

Individuals, roles, or teams are assigned ownership of assets

ICT ensure assets are inventoried

ICT and asset owners ensure assets are appropriately classified and protected

ICT ensure the proper handling when the asset is deleted or destroyed in line with the **ICT 05 Information Classification and Handling Policy**

ICT may delegate routine tasks

Acceptable use of assets

Acceptable use of assets is in line with the **ICT 07 Acceptable Use Policy.**

Return of Assets

All employees and external third-party users must return all organisational assets in their possession upon termination of their employment, contract, or agreement.

Where an employee or external third-party user, purchases organisation equipment or uses their own personal equipment, procedures are in place to ensure all relevant information is transferred to the organisation and securely erased from the equipment.

During notice periods of termination, the council controls unauthorised copying of council information by terminated employees or external third-party users.

Policy Compliance

Compliance Measurement

The service management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Service Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.

Somerset Council

ACCEPTABLE USE POLICY

Acceptable use of assets

Document Owner: [Service Management]

Document Version Control

	Last Modified	Last Modified By	Document Changes
1.0	01/01/2018	P. Grogan	Document first created
1.1	10/03/2022	A. Ware	Updated format and removed reference of any old devices and software.
1.2	19/05/2022	A. Ware	Moved to new template
1.3	04/08/2022	A. Ware	Included new somerset council branding
1.4	22/08/2022	R. Rooks	Final Version for Technology Gateway Panel
1.5	12/01/2023	R. Rooks	SC Branding Applied
1.6	24/02/2023	R. Rooks	Apply updates from LGR HR & Unions review
1.7	15/03/2023	R. Rooks	Official SC Branding & Executive Member Approval

Document Contents Page

Purpose

The purpose of this policy is to make employees and external party users aware of the rules for the acceptable use of assets associated with information and information processing.

Scope

All council employees and external party users.

Acceptable Use of Assets Policy

Principle

Use of assets is in line with applicable legislation, council policies and is in place to safeguard the council data, employees, and customers. Each user is to be responsible for their own actions and act responsibly and professionally.

Individual Responsibility

Access to the IT systems is controlled using a variety of identity methods such as User IDs, passwords, tokens, SmartCards, PINs and Windows Hello for Business (WHfB). All should be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the council IT systems.

Individuals must not:

- Allow anyone else to use their user ID or associated identity methods on any council IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID to access council IT systems.
- Leave any identity method such as password or PIN unprotected (by for example writing them down).
- Perform any unauthorised changes to council IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their role or specific business need to interrogate the system or data.
- Knowingly store council data on any non-authorised equipment.
- Give or transfer council data or software to any person or organisation outside the council without the authority of the council,

Individuals must ensure:

- Line managers where appropriate give clear guidance on the extent and limits of their role and necessary use of IT systems and data.
- All device usage in and away from the office conforms to the appropriate policies for council and personal owned devices

Internet and Online Communication Usage

Use of the council internet and online communications (such as Outlook/Exchange and Teams) is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the council in any way, not in breach of any terms and conditions of employment and does not place the individual or the council in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the Internet and communication systems.

Individuals must **not**:

- Send or store payment information such as:
  - Payment card number (Primary Account Number or PAN)
  - Security code (CVV2 etc.)
  - Start and expiry dates
- Use the Internet or online communications for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which the council considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.
- Use the Internet or online communications to make personal gains or conduct a personal business.
- Use the Internet or online communications to gamble.
- Use the communication systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to the council, alter any information about it, or express any opinion about the council unless they are specifically authorised to do this.
- Send sensitive, internal, or confidential information externally without appropriate protection and the correct sensitivity label.
- Forward council specific rather than user specific sensitive mail to personal (non-council) email accounts (for example a personal cloud or owned domain account) without Information Governance authorisation.
- Download any copyrighted material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Download or install or distribute any software from the Internet without prior approval of the ICT Department.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives are not to be used unless authorised. Only council owned, managed, and authorised mobile storage devices with encryption enabled must be used, when transferring internal or confidential data.

Monitoring and Filtering

All data that is created and stored on council computers is the property the council and there is no official provision for individual data privacy.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The council has the right (under certain conditions) to monitor activity on its systems, including Internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000 and any other applicable legislation.

Reporting

It is your responsibility to report suspected breaches of security policy without delay to your line management, the IT department, the information security department, or the IT helpdesk. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with council disciplinary procedures.

Policy Compliance

Compliance Measurement

The Information Security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement process. It should be updated and reviewed when necessary but no later than 12 months. This process is the responsibility of the document owner.

Somerset Council

CLEAR DESK AND CLEAR SCREEN POLICY

Maintaining a clear desk and clear screen of confidential information

Document Owner: [Service Management]

Document Version Control

	Last Modified	Last Modified By	Document Changes
1.0	10/10/2022	R. Rooks	Branded and updated original template
1.1	12/01/2023	R. Rooks	SC Branding Applied
1.2	24/02/2023	R. Rooks	Apply updates from LGR HR & Unions review
1.3	14/03/2023	R. Rooks	Official SC Branding & Executive Member Approval

Document Contents Page

Purpose

The purpose of this policy is to reduce the risks of unauthorized access, loss of and damage to information during and outside normal working hours.

Scope

All council employees and external third-party users.

All workplace scenarios both inside and outside of official council offices.

Confidential information in electronic and paper form including portable digital media such as USB sticks and drives where permitted.

Monetary items and associated resources.

Clear Desk and Clear Screen Policy

Principle

Clear desk and clear screen are ensuring that resources of value and/or confidential information are secured from unauthorised access, loss, or damage when not in use.

Internal, Confidential and Critical Information

Internal, confidential, sensitive, or critical business information, e.g., on paper or on electronic storage media, should be locked away when not required. Secure lockers or tambours should be provided in the office environment. Ideally a safe or cabinet or desk or other form of security furniture should be used outside the office environment.

Computers, mobile devices, and terminals for individual use should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use. Council devices should automatically lock after 15 minutes of inactivity. For any type of Windows device this can be done immediately by pressing the **Windows Key + L**.

Printers, Photocopiers and Reproduction Technology

Unauthorised use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be avoided and prevented.

Media containing confidential, internal or otherwise sensitive information should be removed from printers and photocopiers immediately.

Cash, Cheques, Bank Cards, Payment Devices

All council related items that are payments or able to take or make payments are to be physically locked away securely when not in use in storage provide by the council.

Media Disposal

Media (as per scope) should be destroyed in line with best and appropriate practice. Internal and confidential council items should be disposed of securely. Where provided for physical media this should be in confidential waste bins or if available shredded (preferably crosscut) and never in general waste.

Policy Compliance

Compliance Measurement

The Information Security Management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement process. It should be updated and reviewed when necessary but no later than 12 months. This process is the responsibility of the document owner.

Somerset Council

MOBILE DEVICE POLICY

Mobile Device Usage

Document Owner: [Service Management]

Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	15/06/2022	S.Ewing	Document first created
0.2	23/06/2022	S.Ewing	Updated to take account of feedback received in workstream meetings to date.
0.2	28/06/2022	S.Ewing	Updated to take account of C+ requirements.
0.3	28/06/2022	S.Ewing	Distributed to district partners for review. Now incorporating feedback received from SWT, Mendip, SSDC
0.4	11/07/2022	S.Ewing	Now incorporating feedback received from SWT, Mendip, SSDC
1.0	09/08/2022	S.Ewing	Approved at Tech Board on 26/07/2022
1.1	15/09/2022	A. Ware	Rebranding with new council logo
1.2	20/10/2022	S.Ewing	Updated to clarify process for using your own device.
1.3	12/01/2023	R. Rooks	SC Branding Applied
1.4	24/02/2023	R. Rooks	Apply updates from LGR HR & Unions review
1.5	15/03/2023	R. Rooks	Official SC Branding & Executive Member Approval

Document Contents Page

Purpose

We recognise that mobile devices have become an integral part of everyday life. They may be a great asset if used correctly (for productivity apps, calendars, business calls etc.)

But mobile devices may also cause problems when used imprudently or excessively and are a security risk should any information, not protected on mobile devices, be accessed inappropriately causing a data breach or safety risk. The purpose of this document is to outline the responsibilities of device owners when using a mobile device either allocated to them by the Council or when using their own device.

All terms must be read and agreed to before devices can be allocated or used.

Scope

This policy applies to:

- All the Council's employees and external party users.
- All the Council's mobile devices.
- All personal devices used to access, process, or store the Council's information.

Mobile devices are to have adequate protection of the Council's information.

Subject to applicable laws and regulations which take precedence employee responsibilities include:

- To ensure the health and safety work environment is consistent with council policy and training at all times and extending to UK law and the use of mobiles.
- To adhere to the Council's policies, including but not limited to:
    - Legal Responsibilities Policy
    - Email Acceptable Use Policy
    - Internet Acceptable Usage Policy
    - Software Policy
    - IT Access Policy
    - Removable Media Policy
    - Information Protection Policy
    - Human Resources Information Security Standards
    - Information Security Incident Management Policy
    - Communications and Operation Management Policy
    - Computer Telephony and Desk Use Policy
    - IT Infrastructure Policy
    - Information Governance Policy
    - Data Protection Breach Policy (appendix C of the Information Governance Policy)
    - Remote Working Policy

Mobile Policy

What is a Mobile Device?

A mobile device is a handheld tablet, phone or network dongle that may require a SIM card (a smart card inside a mobile device, carrying an identification number unique to the owner) for connection to the internet. A mobile device is made for portability and is both compact and lightweight.

Employee Mobile Device Eligibility

Mobile devices are allocated to those that need it most, if you do not fall into one of these categories of employees, you will be required to seek an exception to the policy. Devices and associated equipment, including mobile phones, remain the property of the Council. Please note corporate mobile devices will not be allocated for access control purposes (e.g., Multi-Factor Authentication).

- Frontline worker
- Field worker
- On call
- Lone worker
- Reasonable adjustments.

Mobile Device Registration

- Mobile devices are recorded in the asset register.
- Mobile devices are assigned to a named individual.
- Assigned owners are provided with a copy of the Mobile policy and informed of their responsibility for the device and the information contained on it.
- Mobile devices have appropriate encryption, anti-virus and access control installed, where available.

Mobile Device Assigned Owner Responsibilities

The following are the Council's basic guidelines for proper employee mobile device use during work hours. In general, mobile devices should not be used when they could pose a security or safety risk, or when they distract from work tasks.
Assigned owners are personally responsible for:

- Ensuring that the devices' operating system and application patching is up to date, do not ignore or postpone the update requests received from the provider. Access to applications/ factory reset to devices will be applied if devices become un-supported.
- Ensuring encryption and antivirus, where installed, is enabled
- Ensuring that at a minimum, **all** devices should be screen locked and protected with an eight-digit pin or biometrics.
- Ensuring the device is not left unattended (on a workspace, in a vehicle etc) and when not in use.
- Only accessing the Council's information required for role via the Council's Access Control Policy (i.e., Multi-Factor Authentication).
- Not installing software or change the device that would be in breach of the Council's information security policy, regulations, or applicable legislation. Only download approved applications from the relevant store and or trusted source. Non-council approved mobile applications, music, ringtones, and videos should not be downloaded to any device.
- You should not sign into any application with a Google account or create any Google account on the device for any use. This will lock the device to the account and the device will become unusable if it is re-issued or reallocated later. Any required apps and access will be available by the council play store.
- Ensuring that personal and confidential data is not stored on the device. Council data must *never* be stored on the device memory. All data must be stored within Applications such as OneDrive or SharePoint.
- When accessing the Council data on the device during journeys on public transport or in public places, avoid the risk of unauthorised disclosure of the Council information by a third party overlooking.
- Work emails should only be accessed via the 'Outlook App' and not through the web browser. This is the most secure way and minimises the risk of a data breach.
- You should be mindful of connecting to unsecured, open, or public Wi-Fi. These connections can intercept transmissions including sensitive data and passwords. Be wary of free Wi-Fi offered in public places. Only connect the device to secure Wi-Fi connections.
- Do not hold sensitive conversations about services, staff, or council business in public places.
- Not allowing others including family members to access or use the assigned device or have access to the data held therein. Calls should not contain any language or pictures which may be considered by others to be abusive, obscene, or offensive.
- Take suitable precautions to protect the device. If a device case is provided, the case should not be marked in any way.
- Mobile devices are not to be tampered with in any way.
- SIM cards should not be replaced, changed or altered in any way.

- Returning the mobile device when no longer required, when requested or when leaving the Council's employment, in good condition. If the device is damaged, then the department or the employee will be liable for repairs or a replacement device.
- In the event of loss or theft staff must report this immediately to the ICT Service Desk and the police if appropriate. ICT will charge departments to replace lost devices.
- Never using a mobile device while driving, the Council will not take responsibility for any road traffic violations and fines induced by any employee that chooses to use the corporate device whist driving. The Council will not provide any car peripherals such as hands free kits.
- Never using a mobile device while operating equipment.
- Avoid using work allocated mobile devices for personal tasks.
- Avoid using personal mobile devices for work tasks.
- Avoid using mobile devices during meetings.
- Mobile devices are not to be taken overseas without written authorisation of the Manager.

Line Manager responsibilities:

- Submitting / approving new device requests in line with this policy. Devices are given to those that need it most.
- Managing and monitoring their team's usage via the monthly invoices received.
- Authorising the requests device usage for overseas, following the appropriate Information Governance policy and request process to allow out of country access.
- Ensuring staff comply the mobile policy and reporting non-compliance
- Reporting any suspected breaches of the policy to the ICT department
- Notifying ICT if an employee leaves the Council.
- Approve any user owned device usage
- Returning any device not in use to ICT promptly.

Mobile Remote Wipe or Factory reset.

Mobile devices are enabled to have their contents remotely wiped in the event of loss or theft. This feature is enabled prior to the user being given access to the mobile device or corporate applications and mobile devices have their automatic lockout enabled.

Mobile Back Up

Mobile devices content such as local device settings, photos, text messages and call logs not synchronised with OneDrive are not backed up, it is the responsibility of the assigned user, to ensure the data is secured in the relevant SharePoint folder and synchronised with OneDrive. In event of a device is lost or stolen or factory reset, local data held on devices is lost.

Costs

All Corporate mobile phones supplied by the Council come with a voice & data SIM. Calls to local, national and UK mobile numbers are free with the suppliers call plan. Calls to premium rate 09, Directory Enquiry's and international numbers are barred. Calls to 084 and 087 numbers are not included within the suppliers call plan and charged at 0.6p per min. Calls made outside of the suppliers call plan.

Call costs are charged back to the employee's department.

In most cases corporate devices supplied by the Council come with a 4GB monthly data plan. Some employee's data plans may differ depending on their role. The data plan is for business use only. It is the employee's responsibility to keep within the limit of the monthly data plan. The limit is not capped and therefore going over the limit will cause an immediate additional charge of £50 per month.

If an employee knows they are going to go over the limit and has a justification for doing so, they must agree this first with their line manager. Employee's department will be liable for any additional data costs.

* The mobile devices display the amount of data used per month in real time and the employee can set up data usage limits to notify when a data limit has been reached *

Using your own device

Whether you choose to use your own personal device under a “bring your own device” (BYOD) scheme which is then dedicated for the purposes of conducting the Council’s business or choose to use your own personal device to access work applications like Microsoft Teams, work email, etc “mobile application management” (MAM) scheme, your device will be registered for security purposes.

Background

When using your own device, the Council has ownership of the corporate data and resources that may be accessed on a personal device, the device itself is the property of the user. This means that:

> Council information held in corporate applications available on your device cannot be copied into your personal device and personal information from your personal applications cannot be copied into the Council’s applications.
>
> The Council’s information held in the Council’s applications held on your personal device will fall under the same Security and Information Governance polices as any other Council device owned (E.g., Laptop) and subject to these regulatory and statutory guidance. This includes (but is not limited to) text messages (SMS, MMS and internet based) and camera applications used for the procurement/ processing of data for and behalf of the Council.
> Your personal device (mobile or tablet) will not be managed/changed or interfered with by the Council. Only the Council’s apps that you chose to download to your personal device will be managed by the Council. (A list of apps can be found on the intranet).
>
> It is also important to note that any websites visited, emails, private messages or any information of a personal nature that resides in your personal device and applications are not monitored in any way by the Council.

As devices and platforms have become more capable with being used in a work context, the aim of this initiative is to:

- Give end-users the ability to use device(s) that they feel comfortable with
- Reduce overhead for the procurement and provision of corporate devices
- Enable flexible (including remote) working
- Increase productivity

Where a personal mobile device is used the Mobile Device Assigned Owner Responsibilities apply, in addition:

- The mobile device is recorded in the asset register for security purposes.
- The user receives training and signs an acknowledgement of responsibility.
- All the Council's policies including access control and the information security policy apply.
- The same policy for mobile devices usage (this document) applies.
- Your personal device is compatible with the minimum operating systems requirements
- No Council related data or sensitive data as defined by the GDPR (General Data Protection Regulation) or not suitable for the public domain, or Data Protection Act 2018 is stored on the device.

Process

Users wishing to use their own device can do so by submitting a request through the ITSM Tool, providing the device details and confirmation and acceptance of the mobile policy.

ICT Support

Personally, owned devices are not supported by ICT services. Staff should contact the device manufacturer or their carrier for operating system or hardware-related issues.

The support provided by ICT for personal devices within the BYOD or MAM scheme is limited to:

- Initial user registration
- Remote wiping, of Council Application(s)/ workspace for
    - lost or stolen devices
    - on termination of employment
    - after the agreed number of failed logins attempts to unlock corporate workspace
    - data or policy breach is detected
    - user no longer requires BYOD device with managed Council apps
    - device falls out of compliance (drops below minimum Operating System level required)

  This will only remove the Council's data and will not interfere with any personal content on the device,

Detailed guidance for enrolling your BYOD or MAM is available on the Intranet / Yammer and covers all major functions, including:

- Download and installation of the apps
- Initial registration and set up
- Resetting/re-configuring a device

Policy Compliance

Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance

Improper use of a mobile device, or if found to be in violation of this policy, may result in disciplinary action, up to and including termination of employment. Continued use of mobile devices at inappropriate times or in ways that distract form work may lead to mobile device privileges being revoked.

Mobile device usage for illegal or dangerous activity, for the purposes of harassment, or in ways that violate the Council’s confidentiality policy may result in disciplinary action, up to and including termination of employment.

If a device is returned damaged due to negligence, then the employee will be held responsible for the cost of the device.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement process. It should be updated and reviewed when necessary but no later than 12 months. This process is the responsibility of the document owner.

User Agreement

Before submitting a request for a new mobile device, users must read and confirm they accept the above policy. You will then need to complete your details to request a usage of a corporate device or use of your personal device for BYOD or MAM purposes.

I confirm I will abide by and agree to the following mobile user agreement
Signed:
Date:

Somerset Council

INFORMATION TRANSFER POLICY

Transferring Information

Document Owner: [Service Management]

Document Version Control

	Last Modified	Last Modified By	Document Changes
1.0	01/06/2022	A. Ware	Document first created
1.1	15/08/2022	A. Ware	Included new somerset council branding
1.2	22/08/2022	R. Rooks	Final Version for Technology Gateway
1.3	12/01/2023	R. Rooks	SC Branding Applied
1.4	24/02/2023	R. Rooks	Apply updates from LGR HR & Unions review
1.5	15/03/2023	R. Rooks	Official SC Branding & Executive Member Approval

Document Contents Page

Purpose

The purpose of this policy is ensuring that correct treatment when transferring information internally and externally to the council and to protect the transfer of information using all types of communication facilities.

Scope

All council employees and external third-party users accessing corporate data, no matter how held, by any means, in or from any location.

Information Transfer Policy

Principles

Data transfer must comply with all legal and regulation legislation requirements including but not limited to the GDPR and Data Protection Act 2018.

Formal agreements that include non-disclosure and confidentially clauses must be in place for data sharing prior to the data transfer.

Personal data must not be transferred outside the UK or European Economic Area without legal consent, justification, and legal mechanisms in place.

No personal or confidential information is to be transferred unencrypted.

All transfers are in line with these policies.

Information Virus Checking

Information that is transferred is virus checked where appropriate before being sent or before being opened when received.

Information Encryption

Personal and confidential information is always encrypted before being transferred.

Encryption credentials for username and password where used are shared via two separate and distinct communication methods. The preferred method is to share the username via email and the password via a voice call.

Data Transfer Methods

Preferred Transfer Method

The preferred transfer method is SharePoint.

Access permissions should always be checked and if any doubt the data should be further protected by encryption.

Data Transfer by Email

Email is a suitable solution for transferring information as long as the correct sensitivity level is used. Though it must be borne in mind it is not a guaranteed delivery mechanism and is limited to maximum attachments of 25MB.

Consideration is always given to an alternative secure method of transferring sensitive data or larger quantities of data wherever possible and practicable.

The correct sensitivity level must be chosen where confidentiality must be maintained and should also be set for any attachments where applicable (Office attachments in particular).

Email messages must contain clear instructions of the recipient's responsibilities and instructions on what to do if they are not the correct recipient. By default the standard council footer should cover most circumstances.

Care must be taken as to what information is placed in the subject line of the email or in the accompanying message. Filename or subject line must not reveal the full contents of attachments or disclose any sensitive personal data.

The use of a personal email account for council business is not permitted.

Data transfers by post/courier

Data transfers which occur via physical media such as paper reports, memory cards or CDs must only be dispatched via the council approved secure courier with a record of collection and a signature obtained upon delivery.

The recipient should be clearly stated on the parcel and the physical media must be securely packaged so that it does not break or crack.

The recipient should be advised in advance that the information is being sent so that they are aware when to expect the information. The recipient must confirm safe receipt as soon as the information arrives. The sender responsible for sending the data is responsible for confirming the data has arrived safely.

Data transfers on removable media / memory sticks

Only council owned removable media is to be used for transferring information in line with policy the device usage is approved, recorded in the asset register, assigned, and encrypted.

The removable media must be returned to the owner on completion of the transfer and the transferred data must be securely erased from the storage device after use. The asset register must be updated.

Clear instructions of the recipient's responsibilities and instructions on what to do if they are not the intended recipient must be given. By default this should at least match the instructions sent out by the council on email footers.

Any accompanying message or filename must not reveal the contents of the media.

The process described for **Data transfers by post / courier** must be followed.

Telephones, Mobile Phones and General Conversations

As phone calls (including MS Teams) may be monitored, overheard, or intercepted (either deliberately or accidentally), care must be taken as follows:

- Be conscious of your surroundings especially on public transport such as trains and public places such as coffee shops when discussing personal, confidential, or otherwise sensitive information.
- Personal data must not be transferred or discussed over the telephone unless you have confirmed the identity and authorisation of the recipient.
- When using answer phones do not leave sensitive or confidential messages or include any personal data. Only provide a means of contact and wait for the recipient to speak to you personally.
- When listening to answer phone messages left for yourself, ensure you do not play them in open plan areas which risks others overhearing. Delete them immediately after listening.

Data Transfers over Bluetooth

Bluetooth is not recommended as a communication method for unencrypted confidential, personal, or otherwise sensitive data.

- Ensure device mutual authentication is performed for all accesses.
- Enable encryption for all broadcast transmissions (Encryption Mode 3).
- Configure encryption key sizes to the maximum allowable.
- Establish a —minimum key size for any key negotiation process. Keys should be at least 128 bits long.
- Use application-level (on top of the Bluetooth stack) authentication and encryption for sensitive data communication such as SSL.
- Exercise good practice and encrypt the transfer data anyway regardless of sensitivity.
- Perform pairing as infrequently as possible, ideally in a secure area where attackers cannot realistically observe the passkey entry and intercept Bluetooth pairing messages.
- Note: A “secure area” is defined as a non-public area that is indoors away from windows in locations with physical access controls.
- Users should not respond to any messages requesting a PIN, unless the user has initiated a pairing and is certain the PIN request is being sent by one of the users ‘s devices.
- Use only Security Mode 3 and 4. Modes 1 and 2 should not be allowed. Security Mode 3 is preferred but v.2.1 devices cannot use Security Mode 3.
- Users should not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, or images.
- All Bluetooth profiles except for Serial Port Profile should be always disabled, and the user should not be able to enable them.

Lost or missing information

If it is discovered or suspected that information has been lost, is missing, did not arrive, or has gone to the wrong person then the employee or external party user is required to inform at least one of their line manager, the ICT SOC team, the Management Review team, or the Senior Management team immediately at which point the council Breach Notification Process will be followed.

Policy Compliance

Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement process. It should be updated and reviewed when necessary but no later than 12 months. This process is the responsibility of the document owner.