Gloucestershire County Council
ICT Equipment Policy

1. Policy Statement

Gloucestershire County Council (the council) accepts that ICT equipment is essential to enabling it to meet its aims and objectives. It is a requirement that your use of the council's ICT equipment is legal and appropriate for delivering the council's responsibilities and does not create unnecessary risk. The council will ensure that all users have access to its ICT equipment. **It is a requirement that all users read and accept this policy.**

The council's ICT equipment is made available to users for council business purposes. Limited personal use is permitted provided that such use is strictly in accordance with this policy, which can be found at Information Management and Security Policies.

2. Risk Management

The council recognises that there are risks associated with use of ICT equipment.

This policy aims to ensure appropriate access to, and use of, the council's ICT equipment, which will help to mitigate the following risks:

- Harm to individuals
- Damage to the council's reputation
- Potential legal action and/or fines against the council or individual(s)
- Inappropriate use of council resources
- Viruses and other malicious software
- Service disruption

3. Scope

This policy applies to all users of the council's ICT end user devices. This includes, but is not limited to:

- Desktops and laptops,
- Mobile devices, e.g., mobile phones and tablets,
- Portable media devices, e.g., memory sticks, external hard drives, DVDs,
- Agile working equipment.

All users are expected to comply with this policy at all times when using the council's ICT equipment, whether accessed locally or remotely (e.g., via the council's Remote Access Gateway, or via any council owned device). Breach of this policy may be dealt with under the council's Disciplinary and Dismissals Procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal.

4. Responsibilities

The Assistant Director: Digital & ICT has overall responsibility for the effective operation of this policy. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to the council's operations lies with the Senior Information Risk Owner. If you do not understand the implications of this policy or how it may apply to you, you should seek advice from Service Now.

The council will:

- Ensure that end user devices (including laptops) are protected using approved encryption software.
- Provide and install authorised encrypted memory sticks (these are only available by exception and must be purchased and installed by ICT).
- Ensure software is available to encrypt content on portable devices.
- Apply port security to end user devices to ensure that data can only be written (saved) to approved encrypted devices.
- Ensure Microsoft end point protection is enabled on all end user devices.

All managers have a specific responsibility to comply with this policy, ensure that all users understand the standards of behaviour expected of them, and to act when behaviour falls below these requirements.

Heads of Service are responsible for the following:

- Ensuring budget holders understand their responsibilities in approving requests for end user devices in their area, and the payment of any charges incurred.

Line Managers are responsible for:

- Ensuring that the billing name correctly represents the user of any mobile device and/or data SIM and that the cost code associated with the device is accurate.
- Ensuring that when a member of staff leaves, the appropriate leavers procedure is adhered to so that end user devices are promptly returned to ICT and all relevant records/contracts are updated.
- Raising concerns around excessive personal use of corporate mobile phones with the ICT Service over and above any inclusive minutes included in the data allowance. Staff found to be using their devices inappropriately will be subject to disciplinary procedures.

All employees and anyone who delivers services on the council's behalf e.g. contractors, partners, agents or other third parties with access to the council's information assets have a responsibility to comply with this policy which can be found at Information Management and Security Policies.

All users of ICT equipment should be aware that their use of the council's systems can be monitored, and where breaches of this policy are found, action may be taken under the council's Disciplinary and Dismissals Procedure. The council reserves the right to restrict or prevent access or introduce routine monitoring if personal use is considered to be excessive.

Under no circumstances should an employee use a personal device, other than those approved under BYOD, for any work purposes.

5. User Responsibility

Use of all ICT equipment must be consistent with the council's Code of Conduct for Employees. All users are responsible for using the council's ICT equipment appropriately and in accordance with the statements in this policy.

It is the user's responsibility to:

- Ensure they read, understand, and agree to this policy.
- Use the council's ICT equipment in accordance with the terms of this policy and in a way that will not harm the council's reputation.
- Recognise that the council's ICT equipment is provided for business use and must be protected from unreasonable and excessive personal use.
- Report any misuse of the Council's ICT equipment by following the council's security breach reporting procedure.

6. Related policies

- Code of Conduct for Employees
- Internet and Digital Communications Policy
- Information Protection and Handling Policy
- Information/IT Access Policy
- Information Security Policy
- Data Protection Policy
- Software Management Policy
- Social Media Policy
- Password Policy

The above policies are available at Information Management and Security Policies.

7. Things You Must Do

When using the council's ICT equipment, you **must**:

a. **Security controls and use of your account details**

- ✓ Promptly respond to any requests from ICT to carry out remedial action to your laptop if it fails to update.
- ✓ Keep a separate record of the asset tag of the device in the event of loss or theft.
- ✓ Keep your mobile device(s) in a secure location when not in use. Carry and store your device(s) in a suitable padded bag to reduce the chance of accidental damage.
- ✓ Immediately report any suspected or observed security breach thorough the council's security breach reporting procedure.

b. Encryption

- ✓ Use council approved security software to encrypt personal, special category or other sensitive information in transit (email).
- ✓ Ensure compliance with the council's Password Policy at all times.

c. Contact Service Now if you encounter any issues with the device's encryption software, for this to be resolved.

Information and content:

- ✓ Take extra care when opening email attachments (the number one source of computer viruses). Email attachments should not be opened unless the email comes from a trusted source and/or you were expecting it.
- ✓ Assess your working environment and ensure appropriate security regardless of whether you are in the office, at home, in any other location or whilst travelling.

8. Things you Must Not Do

When using the council's ICT equipment, you must **NOT**:

a. Security controls and use of your account details:

- ✘ Disable, defeat or circumvent any security measure that the council has put in place to protect its information assets, physical assets or reputation.
- ✘ Keep encryption passwords and logon credentials with your device or share them with your colleagues.
- ✘ Use ICT equipment for anything other than official council business and not for generating, transmitting or delivering any content that is contrary to council policies.
- ✘ Leave ICT equipment unattended at any time when outside council premises including, but not limited to, in a car, briefcase or handbag. If it is absolutely necessary to temporarily store your device(s) in a car, it should be locked out of sight in the boot or other compartment, **but it is generally much safer to take it with you**.
- ✘ Leave your laptop unattended and logged on. If not in use, it should be locked, logged out and shut down.
- ✘ Use ICT equipment not procured through the ICT service to store, use or transfer any council information.
- ✘ Use GCC mobile devices for any personal phone calls.

b. Access:

- ✘ Allow your ICT equipment to be used by work colleagues, family members, friends or visitors – all staff are personally accountable for anything accessed via their user ID.
- ✘ Use any damaged or faulty ICT equipment.
- ✘ Transfer data using portable media, unless authorised.

c. Copyright:

- ✘ Download or install any unauthorised accessories or software programs as per the council's Software Management Policy, including software that allows the device to be remotely controlled or that helps diagnose or resolve issues (e.g. network sniffers and password crackers).

d. Information and content:

- ✘ Send personal or special category information to a non-GCC email account or transfer it to removable media (including encrypted USB drives) for the purposes of remote working.

- ✘ Process **any** council information on a non-GCC device.
- ✘ Send personal, special category or other business-related data via any Internet service(s) not supplied by the council without relevant permission.

9. Procurement of ICT equipment

All ICT equipment, including portable media devices such as USB memory sticks and cameras must be purchased and installed via Service Now. All ICT equipment will be recorded on the ICT Asset Register. Equipment must display a GCC asset tag and will remain the property of GCC at all times. Devices may be updated, replaced or removed as appropriate according to users' ongoing requirements or council policy.

10. Approved GCC Remote Working Solutions

The Council's remote access gateway solution enables access to the council network and the same information you would normally access from council premises. It provides remote access to systems and data in a controlled way to minimise risk. All information is created, stored, and processed on council servers, not the local hard drive of the machine being used for access.

Before allowing access, the remote access software will check to ensure the connecting device is authorised, and its software is up to date. If the connecting device fails these tests, access will be denied.

Personal devices are not able to access the council's remote access gateway and therefore must not be used to process council data under any circumstances.

A council-owned, encrypted laptop may be used as a standalone device where access to the network is not available. Personal or special category (sensitive personal) information relating to individuals in receipt of support/services from the council must be added to their individual record (e.g., on Liquid Logic) in a timely manner, preferably on the same day but no later than 3 days after the event.

The council's mobile device management solution may (subject to eligibility and conditions for use) be used with a user-owned personal device such as a smart phone or tablet device to access council email, contacts, calendar and Staffnet via the device's 4G service or Wi-Fi. This is the councils only approved 'Bring Your Own Device' (BYOD) solution. Further information can be found by via the Blackberry Work staffnet page.

11. Third Party External Access to the Council's network

External access to the council's network for partners, contractors, agents or other third parties must be via the remote access gateway, using an organisationally owned PC/laptop with up-to-date anti-virus software, supported operating system and from within the European Economic Area or a country with an approved adequacy agreement in place.

Third parties must confirm that a regular patching process (no less than monthly) is in place within their organisation and is being followed. Failure to comply with this process, leading to the introduction of malicious code onto GCC systems, will result

in the right to use the system being removed immediately and legal action may be taken.

Third parties must confirm that disk encryption is in place on the corporate end user device which is being used to access the GCC network. They must also have a clear process in place for dealing with lost or stolen devices, which ensures that all information on the device can be wiped remotely.

12. Restricted Use of Portable Media

Portable media includes, but is not restricted to the following:

- USB Memory Sticks (also known as pen drives or flash drives)
- CDs
- DVDs
- Optical Disks
- External Hard Drives
- Digital Cameras
- Audio Tapes (including Dictaphones and Answering Machines)

It is the council's policy to minimise storing personal or special category information directly onto portable media. There are a number of council approved solutions to this, please contact ICT to discuss the options available to you.

Users should be aware that the council may, as and when required, and without the permission of the relevant user, audit/log the transfer of data files to and from all portable media devices and council-owned ICT equipment.

13. Transferring data using portable media

Anyone using portable media to transfer data must ensure that they are authorised to do so (bulk transfers of data require the appropriate Information Asset Owner's approval), and take care to physically protect the portable media and stored data from loss, theft or damage. They must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Up-to-date virus and malware checking software must be in place when portable media devices containing personal or special category information are connected to another device i.e. both the device from which the data is taken and the device to which the data is being uploaded.

Data stored on portable media may not be included in the council's backup process; therefore, there is a greater risk that the information will become unavailable through loss or malfunction of equipment. Source data should remain on the council's network at all times, and any business-critical data created or originating on portable media should be transferred to the council's network as soon as possible.

Portable media devices should not routinely be used for archiving or storing records as an alternative to other storage equipment. Where this is necessary it should be approved by the Information Asset Owner following completion of a risk assessment.

14. Recording of Electronic Communications on Case Files

Where council mobile devices are used for electronic communication with service users, all council policies for record keeping still apply, regardless of whether communications are sent or received. These communications include, but are not limited to:

- Phone calls
- Emails
- Voicemails
- Text messages
- Messages sent via social media e.g., Facebook
- Messages sent via an instant messaging service e.g., WhatsApp

This means that any such communication should be recorded as professional contact within the relevant records. The record should include the message (as accurately as possible to reflect its content), date and time, and details of the sender and recipient (e.g., mobile number). Messages or other correspondence should then be deleted from the mobile device to maintain confidentiality.

Staff should remember that all contact with service users must be regarded as professional contact. Judgement must be exercised when responding to communications using mobile devices, regardless of the format in which it is received.

15. Returning/disposal of ICT equipment

Any ICT equipment no longer needed by a user should be returned to ICT within 30 days. If the user is leaving the council permanently then this must be in line with the Leavers procedures, and a SAP Leavers Form must be completed. Further information or advice is available from the ICT Service.

Disposing or returning GCC Mobile Communication Devices

- Staff leaving the council will not be permitted to transfer their council mobile number to a personal device. If the device has not been returned within one month of the employee leaving or becoming declassified as an essential user, legal action will be taken against the individual.
- If staff are not going to use their council mobile for more than 30 days (e.g., due to holiday, sick leave, maternity leave, etc.) or are suspended from work for whatever reason, they must inform their line manager who will arrange for the device to be collected and returned.

Disposing of Portable Media Devices

- The contents of any reusable media that is no longer required by the council must be erased.
- Portable media devices must be disposed of securely via the ICT Service. Users are responsible for secure delivery of the portable media to the ICT Service for destruction.

16. Exceptions

Memory Sticks:

- Any deviation requires an authorised business case which clearly demonstrates that the risks associated with the use of unencrypted portable media are outweighed by the business benefits, and that appropriate actions have been taken to minimise these risks. Further information about port security can be found by contacting the ICT Service.
- Security controls exist to disable downloading data to portable media by default (except for approved devices e.g., encrypted Safesticks) – if you have a business justification to do this, you will need to apply for a Port Security Exemption to enable this functionality, subject to authorisation by the relevant Information Asset Owner.

Calls to International or Premium Rate Numbers:

- Managers who have authorised calls to Premium Rate and/or international numbers must be aware of the costs that they are incurring.
- Managers who have authorised calls to Premium Rate numbers must ensure that they review this on at least a quarterly basis.

17. Policy Compliance

Security breaches that result from a deliberate or negligent disregard of any security policy requirements may, in the council's absolute discretion, result in disciplinary action being taken against that employee. In the event that breaches arise from the deliberate or negligent disregard of the council's security policy requirements by a user who is not a direct employee of the council, the council shall take such punitive action against that user and/or their employer as the council in its absolute discretion deems appropriate.

The council may, in its absolute discretion refer the matter of any breach of its security policy requirements to the police for investigation and (if appropriate) the instigation of criminal proceedings, if in the reasonable opinion of the council such a breach has or is likely to lead to the commissioning of a criminal offence.

18. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

Document Control

Author:	Peter Moore, Information Management Service
Owner:	Karl Grocock, Assistant Director: Digital & ICT
Document Number:	v2.0

Revision date	Summary of Changes	Changes marked
October 2018	Incorporated Laptop, Mobile Device Portable Media and remote Working Policies into new ICT Equipment Policy, major update of generic content, updated hyperlinks and references to DPA1998 to GDPR and DPA 2018	1.0
March 2019	Review of section 8 – 'Things you must not do'	1.1
September 2021	Minor changes for accessibility purposes including change of policy owner.	1.2
March 2022	Major review and change of policy owner	2.0

Document Approvals

Version	Approved by	Date
1.0	Information Board	December 2018
2.0	Information Board	March 2022