Gloucestershire County Council
ICT Equipment Policy

1. Policy Statement

Gloucestershire County Council (the Council) accepts that ICT equipment is essential to enabling the Council 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 equipment. ICT equipment includes, but is not limited to:

- Laptops,
- Mobile devices, e.g. mobile phones and tablets,
- Portable media devices, e.g. memory sticks, external hard drives, DVDs, and,
- Remote 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 Council's Director: Strategy & Challenge 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 Head of ICT. If you do not understand the implications of this policy or how it may apply to you, you should seek advice from the ICT Service Desk.

The council will:

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

All managers have a specific responsibility to operate within the boundaries of this policy, ensure that all users understand the standards of behaviour expected of them, and to take action when behaviour falls below these requirements.

Heads of Service are responsible for the following:

- Approval of requests for Mobile Communication Devices in their area, and the payment of charges incurred signing off a formal request for a Mobile Communication Device if their approval is granted. This signed formal request must be received by the GCC FM supplier before the Mobile Communication Device is ordered.
- Reviewing the current use of Mobile Communication Devices in his or her area before approving new requests. The review should consider the appropriateness, affordability and the process by which use of the Mobile Communication Devices will be managed.

Line Managers are responsible for:

- Ensuring that the billing name correctly represents the user of the Mobile Communication Device and that the cost code associated with the device is accurate. This includes where the device is allocated to a secondee. Where a device is shared, the billing name must be the person who is responsible for the device.
- Ensuring that when a member of staff leaves the appropriate leavers procedures are adhered to so that Mobile Communication Devices are returned to GCC and all relevant records/contracts are updated.

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 all 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 to certain ICT equipment or introduce routine monitoring if personal use is considered to be excessive.

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 as part of their induction to the Council;
- Use the Council's ICT equipment in accordance with the terms of this policy;
- Use the ICT equipment responsibly and in a way that will not harm the Council's reputation;
- Recognise that the Council's ICT equipment facilities are provided for business use and must be protected from unreasonable and excessive personal use;
- Report any misuse of the Council's ICT equipment. Details of how to do this are provided here;

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

- ✓ Ensure that the council anti-virus software and security patches are updated on the laptop on a regular basis. Laptops must be regularly connected to the internet and at least once a week if staff work predominantly offline (requires a connection to the internet or the GCC data network). Keep a note of the make, model, serial number and asset number of the laptop in the event of an incident (not stored with the laptop).
- ✓ Make backups of data when working offline by utilising the 'P' Drive synchronisation ability, or if access to the Council network is not possible to encrypted CD/DVD or USB memory sticks, etc.
- ✓ Keep personal use of ICT equipment to a minimum.

- ✓ Lock your laptop away out of sight when not in use, preferably in a lockable cupboard, filing cabinet or safe (this also applies out of the office where possible).
- ✓ Carry and stored your laptop in a suitable padded carry bag (preferably unbranded) or strong briefcase 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 the council's approved encrypted memory sticks (Safestick), unless otherwise authorised (see section 8).
- ✓ Use Egress or other approved security software to encrypt personal, special category or other sensitive information on portable media.
- ✓ Ensure the laptop encryption is in use.
- ✓ Use strong encryption password / phrase / pin numbers in line with Council's Password Policy.
- ✓ Contact the ICT Service if you are using a Council owned device which is not enabled for encryption, in order for this to be resolved.

c. Access

- ✓ Ensure that if your role dictates, you are contactable via any GCC mobile communication device (i.e. mobile phones) you are issued with during business or call-out hours, except when driving or when the circumstances deem it inappropriate to do so.
- ✓ Contact the ICT Service Desk immediately if you receive a suspected virus or if you experience any unusual occurrences in respect of the Council's ICT equipment (e.g. an antivirus software warning).
- ✓ If you connect via remote access, ensure you use the Pink Layer connection as this will synchronise your 'P' drive data back to the main server, mitigating the requirement to use portable storage devices.

d. Information and content:

- ✓ Keep calls from a mobile device to a minimum and, wherever possible, use a landline.
- ✓ 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.
- ✓ Take account of the environment you are working in and ensure adequate security regardless of whether the laptop is used in the office, at home, in any other location or while travelling.

8. Things you Must Not Do

In using the Council's internet and digital communications facilities you must **NOT**:

a. Security controls and use of your account details:

- ✘ Disable, defeat or circumvent any security measure that GCC has put in place to protect the information assets, physical assets or reputation of the Council.

- ✘ Keep encryption passwords and logon credentials with the laptop, and do not share them with any 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 GCC premises including, but not limited to, in a car, briefcase or handbag. If absolutely necessary to store in a car, equipment 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 or 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 – 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 (see section 8)

c. Copyright:

- ✘ Download or install any unauthorised accessories or software programs as per the council's Software Management Policy, including software that allows the laptop to be remotely controlled and software 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 transferred to removable media (including encrypted USB drives) for the purposes of remote working.
- ✘ 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 by the ICT Service. 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 (NetScaler) 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. Where there is a business need for remote access further information and an application form is provided here.

Access must be via a device which meets the criteria of NetScaler. Before allowing access NetScaler will check to ensure the connecting device is an authorised device, and that software on the connecting device meets the required standards. If the connecting device fails these tests access will be denied.

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. Liquid Logic/Eric) in a timely manner no later than 3 working days after the event and preferably on the same day.

The Council's mobile device management solution (Blackberry Work) 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 4G service or Wi-Fi. This is the Council's only approved 'Bring Your Own Device' (BYOD) solution. Further information is available here.

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 NetScaler, 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 predefined friendly state.

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 is wiped clean.

12. Restricted Use of Portable Media

Portable media include, but are 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
- Backup Cassettes
- 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. Where this is unavoidable the information must be protected by encryption. Encrypted USB Memory Sticks are available from the ICT Service.

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 sensitive information are connected to a machine i.e. both the machine from which the data is taken and the machine to which the data is to be loaded.

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; 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 a risk assessment.

14. Recording of Electronic Communications on Case Files

Where GCC Mobile Communication Devices are used for electronic communication with service users, 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 internet 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 the content of the message), 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 phone 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 the user should be returned to ICT as soon as possible. If the user is leaving the council permanently then this must be in line with the Leavers procedures, and a SAP Leavers Form completed. Further information or advice is available from ICT Service Desk.

Disposing or returning GCC Mobile Communication Devices

- Staff leaving GCC will not be permitted to transfer their GCC Mobile Communication Device number to a personal device. If the device has not been returned within one month of the employee leaving or of the employee becoming declassified as an essential user, legal action will be taken.
- If staff are not going to use their GCC Mobile Communication Device for more than 30 days (e.g., 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 Mobile Communication Device to be collected.

Disposing of Portable Media Devices

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

16. 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 the Council's 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 breach has or is likely to lead to the commissioning of a criminal offence.

17. 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 the risks. Further information about port security is provided at here.

- 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:

- Lifting the bar on international calling; Line Managers who have authorised international calling must review this on at least a quarterly basis.
- Calls to Premium Rate numbers (such as '0898' numbers); Line Managers who have authorised calls to Premium Rate numbers must ensure that they review this on at least a quarterly basis.

Personal calls:

- For staff travelling outside the UK on GCC business an allowance of £15.00 is paid in the month of the journey for private calls. This allowance applies to both pool and non-pool 'phones and accounts for the additional costs incurred for non-UK usage for both incoming and outgoing calls, messages etc.

18. Review and Revision

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

19. Document Control

Author:	Peter Moore: Information Management Service
Owner:	Jane Burns, Director: Strategy & Challenge (Chief Information Officer and Senior Information Risk Owner)
Document Number:	V1.1

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	V1.0
March 2019	Review of section 8 – 'Things you must not do'	V1.1

Document Approvals

Version	**Approved by**	**Date**
Version 1.0	Information Board	December 2018
Version 1.1		