Gloucestershire County Council
Members ICT Equipment (Acceptable Use and Disposal) Policy

Policy Statement

1. Gloucestershire County Council (the council) accepts that ICT equipment is important in enabling councillors to fulfil their role. Councillors' use of the council's ICT equipment must be legal and appropriate and not create unnecessary risk. The council will ensure that all councillors have access to appropriate ICT equipment and it is a requirement that all councillors read and accept this policy.

2. ICT equipment is made available to councillors primarily to support their elected role. Limited personal use is permitted so long as this strictly follows this acceptable use policy.

Scope

3. This policy applies to councillors who use council issued ICT equipment, including desktops, laptops, tablets etc., and must be complied with at all times when using such equipment (see Appendix 1).

Risk Management

4. There are risks associated with the use of ICT equipment, and the extensive damage that can be caused by misuse. This policy aims to ensure appropriate access to, and use of the council's ICT equipment to help 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

People responsible for implementation of this policy

5. The council's Director of Policy, Performance & Governance 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 Assistant Director of ICT (in consultation with the Head of Democratic Services and the Head of Information Management).

6. If you have any questions about this policy or how it may apply to you, you should seek advice from Democratic Services or the ICT Critical Users Service.

7. Councillors 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 by the council's Monitoring Officer. The council reserves the right to restrict or prevent access to certain ICT equipment or introduce routine monitoring.

Member Responsibility

8. You agree to:
    a. Ensure you read, understand and abide by this policy.
    b. Use the council's ICT equipment appropriately and in accordance with the terms of this policy.
    c. Use the council's ICT equipment responsibly and in accordance with your responsibilities as a county councillor.
    d. Recognise that council ICT equipment is primarily provided for business use and must not be subject to unreasonable and/or excessive personal use.
    e. Be aware that any council information, no matter what device it is held on, is subject to the Freedom of Information Act, 2000 and the Environmental Information Regulations, 2004.
    f. Report any misuse of the council's ICT equipment to Democratic Services or the ICT Critical Users Service.
    g. Ensure that ICT equipment is not left unattended at any time 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).
    h. Ensure that when you stop being a county councillor, all allocated ICT equipment and accessories are promptly returned to Democratic Services.
    i. Promptly report any loss or theft of any council asset to Democratic Services. If it is possible that information has been lost or compromised you must also inform Democratic Services who will report this as a potential information security incident.
    j. Be aware of related council policies including:
        - Members Code of Conduct
        - Information Protection and Handling Policy
        - Internet Acceptable Use Policy
        - Information/IT Access Policy
        - Data Protection Policy
        - Software Management Policy
        - Members Social Media Policy
        - Password Policy

        Generic policies are available at Information Management and Security Policies. Member-specific policies and guidance can be found in Members Matters.

9. Members must not disable, defeat or circumvent any security measures put in place to protect council ICT equipment issued to them.

10. To ensure continuing compliance with the General Data Protection Regulation (GDPR), it is the council's policy to minimise the use of portable media (e.g. memory sticks, tablets, external hard drives) for storing personal or special category information. Special category information includes (but is not limited to) an individual's race, ethnic origin, political beliefs, religion, health conditions or sexual orientation. Where this is not possible, all personal or special category information held on portable media **must** be encrypted. Councillors accessing or storing personal or special category information using their iPad must only do so via the secure Blackberry Work App.

11. Emails relating to council business must be sent from within BlackBerry Work or directly from the council's Outlook email. This ensures appropriate levels of security are applied, where necessary, and that information is sent to recipients safely, securely and in line with all relevant legislation and regulations.

12. In exceptional circumstances, the council reserves the right to access data from all portable media devices and council-owned ICT equipment without the permission of the user. In line with the Council's arrangements for dealing with allegations of member misconduct, any such access must be authorised by the Monitoring Officer.

Registration of ICT equipment

13. ICT will maintain a record of all physical ICT assets held by the council. 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 councillors' ongoing requirements or council policy.

Policy Compliance

14. Any breach of the council's security policy requirements may be considered under the Member Code of Conduct and, where appropriate, the relevant group leader will be informed. This may result in the withdrawal of IT services or, in exceptional circumstances, be referred to the Information Commissioner's Office or the police for investigation, and (if appropriate) the instigation of criminal proceedings, if such breach has or is likely to lead to the commissioning of a criminal offence.

Review and Revision

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

Document Control

Author:	Kirsty Benzie Information Management Service
Owner:	Rob Ayliffe: Director of Policy, Performance & Governance (Monitoring Officer, Senior Information Risk Owner)
Document Number:	V1.1

Revision date	**Summary of Changes**	**Changes marked**
May 2021	Updated to reflect change in document owner	1.1

Document Approvals		
Version	**Approved by**	**Date**
Version 1.0	Jane Burns	15th March 2019
Version 1.1	Rob Ayliffe	22nd April 2021

Appendix 1 – Member Responsibilities

a) Use

- Council provided ICT equipment is only to be used in the course of official council business. Limited personal use is also permitted in accordance with this policy.
- Members should never leave their device unattended and the screen unlocked. If not in use, the screen should be locked or the device should be powered off.
- Your device should not be used by work colleagues, family members, friends or visitors. Members are personally accountable for anything accessed via the device registered to them.
- Members must not download or install any unauthorised Apps. If Members require an app that is not currently available, they should raise this with Democratic Services who will liaise with ICT to assess the compatibility/security of the app.
- Members should not store or download large quantities of media files (e.g. photos and/or music) on the device registered to them.
- Members should always use the Blackberry Work app to store or access personal or special category data via their device and to send emails relating to council business.

b) Storage

- Members are responsible for taking account of the environment they are working in and providing adequate security regardless of whether the device is used in the office, at home, in any other location or while travelling.
- Your device should be locked away out of sight when not in use, preferably in a lockable cupboard, filing cabinet or safe (this applies at home, in the office or in a hotel).
- Your device should be carried and stored in a suitable bag (preferably unbranded) to reduce the chance of theft or accidental damage.

c) Passwords

- Your device must be protected using the Council's approved encryption software and a long, strong encryption password/phrase/pin number in line with council policy. These should be kept secure and not shared or stored with the iPad.

d) Cyber Security

The ICT Service have implemented several layers of protection against all forms of malware and viruses which are a continuing and ever changing major threat to valuable organisational data. Councillors must therefore ensure that they always comply with the following actions in order to safeguard council systems and data:

- Take extra care when opening email attachments (the number one source of computer viruses). Email attachments or hyperlinks within emails should not be opened unless from a known/trusted source.
- Promptly report any loss, theft or compromise of equipment or data to Democratic Services
- Promptly report warning messages or unusual functioning (e.g. unusual file activity) to the ICT Critical Users Service. Files should not be forwarded nor any data uploaded onto the network if you suspect your device might be infected – seek advice from the ICT Critical Users Service first.
- Do not download freeware, shareware or other internet 'apps' as these are a common source of malware infection.