information management & security

Gloucestershire COUNTY COUNCIL

Elected Members ICT Equipment & Information (acceptable use and disposal) Policy

1.0 Policy Statement

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

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

As part of your role as a county councillor you will also have access to council information. This policy sets out the standards for the use of that information, by promoting secure working practices that help to minimise the risk of loss or disclosure.

2.0 Scope

This policy applies to Members (county councillors) who have access to council information and use council issued ICT equipment, including desktops, laptops, tablets etc.; it must be complied with at all times(see Appendix 1).

3.0 Risk Management

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

4.0 Responsibilities

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 Digital & ICT (in consultation with the Head of Democratic Services and the Head of Information Management).

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

4.1 Member Responsibility

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 Critical User 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. Not disable, defeat or circumvent any security measures put in place to protect council ICT equipment issued to you.
i. Ensure that when your term as a county councillor comes to an end, all allocated ICT equipment and accessories are promptly returned to Democratic Services.
j. Promptly report any loss or theft of council equipment 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.
k. 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

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

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.

5.0 Information & content

It is important that council information is not accessed by anyone that does not have a right to see it, therefore Members are required to ensure that their working environment is secure, and that their ICT equipment is locked or powered down when unattended or not in use.

Emails containing council information should not be auto-forwarded to any personal/non-GCC email accounts; manual forwarding is permitted if the email does not contain any personal, special category or commercially sensitive information pertaining to the council.

Storage of corporate information should be on the appropriate SharePoint site, whilst Members should save all others documents on their OneDrive.

Printing council information should be avoided where possible, but if printing is necessary any paper records containing personal, special category or commercially sensitive information must be stored securely in a lockable cabinet or drawer.

Disposal of any paper records containing council information should be done using a cross-cut shredder or by returning to the council for secure disposal.

6.0 Registration of ICT equipment

ICT will maintain a record of all physical ICT assets held by the council. Equipment must display an appropriate asset tag and remains the property of the council at all times. Devices may be updated, replaced or removed as appropriate according to

Members' ongoing requirements or council policy.

7.0 Policy Compliance

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 a breach has or is likely to lead to the commission of a criminal offence.

8.0 Monitoring and review

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

9.0 Document Control

9.1 Document information

Owner:	Director of Policy, Performance & Governance (Monitoring Officer, Senior Information Risk Owner)
Author:	Kirsty Benzie, Assistant Head of IMS
Reviewer:	Kirsty Benzie, Assistant Head of IMS
Board(s) consulted:	
Date created:	March 2019
Next review date:	March 2028
Approval:	Jenny Grodzicka Head of Information Management & Emergency Planning
Date of approval:	April 2025
Scheme of Delegation ref:	DPPG1
Version:	2.0
Classification:	UNCLASSIFIED

9.2 Version History

Version	Version date	Summary of Changes
1.0	March 2019	First version
1.1	May 2021	Updated to reflect change in document owner
1.2	July 2021	Minor changes for accessibility purposes
1.3	July 2024	Updated to reflect change from Blackberry Work to O365
1.4	September 2024	Accessibility review and updates to formatting. Broken links fixed. Removed paragraph referring to portable

		media, memory sticks, tablets, external hard drives etc as these are not issued.
2.0	March 2025	Review in line with all Member-specific policies. Combined with Elected Members Information Security Protocol to create one policy.

9.3 Review

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

9.4 Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Email: dpo@gloucestershire.gov.uk

Phone: 01452 324000

Appendix 1 – Member Responsibilities

Use

a. 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.
b. Members should never leave their device unattended, and the screen unlocked. If not in use, the screen should be locked (using the Ctrl, Alt and Delete keys or Windows and L shortcut keys), or the device should be powered off.
c. Your device should not be used by work colleagues, family members, friends or visitors. Members are personally accountable for anything accessed via any device registered to them.
d. Members must ensure that council information is not accessed by anyone who does not have a right to see it.
e. Members must not download or install any unauthorised applications or software. If Members require something that is not currently available, they should raise this with Democratic Services who will liaise with the Digital & ICT Service to assess its compatibility/security.
f. Members should not store or download large quantities of media files (e.g. photos and/or music) on any council device registered to them.

Storage

a. Members should use the SharePoint site they have access to for storing corporate information, and their OneDrive to store personal documents.
b. Members should have a lockable filing cabinet or drawer for personal, special category or commercially sensitive paper records.

Security

a. 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. This includes ensuring that you are not overlooked when working on your device, and ensuring personal, special category or commercially sensitive information is not accessible to others.
b. Members can safely use public WiFi to access the council's Microsoft tenancy as the associated Virtual Private Network (VPN) enables the encryption of data over a secure connection.
c. 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).
d. Your device should be carried and stored in a suitable bag (preferably unbranded) to reduce the chance of theft or accidental damage.

Passwords

a. 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 stored securely away from the device and not shared.

Cyber Security

The Digital & 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. Members must therefore ensure that they always comply with the following actions in order to safeguard council systems and data:

a. Take extra care when opening email attachments or clicking on hyperlinks within emails if you are unsure of their origin or they are not from a known/trusted source.

b. Promptly report any loss, theft or compromise of equipment or data to Democratic Services.

c. Promptly report warning messages or unusual functioning (e.g. unusual file activity) to the 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 Critical Users Service first.

d. Do not download freeware, shareware or other internet 'apps' as these are a common source of malware infection.

e. Avoid entering your council email address on commercial or non-secure websites, because as well as being a security risk, it can also increase the SPAM/junk mail you receive.

f. Don't do anything to jeopardise the council's or a third party's confidential information through the use of social media, e.g. Facebook, Instagram, X or TikTok.

E-learning

a. Members are responsible for completing their cyber security e-learning in a timely manner and should check for updates and new releases on a regular basis. Please use this guidance document to access the e-learning on the MyCompliance website.