Bring Your Own Device (BYOD) Policy

An accessibility friendly version of this policy is available on the Information Management and Security Policies page.

1.0 Policy Statement

Gloucestershire County Council (the council) has a responsibility to ensure that its information assets are protected and access controlled to maintain the confidentiality and integrity of that information. The council also accepts that to promote hybrid and flexible working there is a requirement for staff to have access to information and systems from personal devices using the council's approved Bring Your Own Device (BYOD) technology.

The purpose of this policy is to define accepted practices, responsibilities and guidance for the use of approved personal devices that the council authorises to connect to its systems. It also aims to ensure appropriate access and use of council information and systems, which will help to mitigate against:

- Harm to individuals
- Loss of personal, special category, commercial or politically sensitive data
- Damage to the council's reputation
- Potential legal action and/or fines against the council or individual(s)
- Inappropriate use of council resources and systems
- Viruses and other malicious software
- Service disruption

This policy also sets out how the council will control access to council systems and information on personal devices in order to support compliance with Cyber Essentials standards. It is important that the consequences and obligations of this arrangement are well communicated and understood.

Any suspected or observed breach must be promptly reported in line with the council's Information Security Incident Management Policy.

BYOD is provided to staff employed by the council, and therefore they must read and accept this policy upon first accessing any data or systems via the BYOD system.

2.0 Scope

This policy applies to all employees, partners, contractors, Members, agents of the council and other third parties (‘users’) who use personally owned or unmanaged internet connected devices to connect to GCC systems.

All council data accessible on a user’s device via BYOD remains the property of the council.

3.0 Eligible devices and platforms

BYOD will be accessible to staff on all internet connected compatible devices (for example, Apple, Android or Windows devices). Unmanaged and unapproved printers must not be used to print GCC data.

BYOD access is limited to M365 apps and selected externally hosted systems that support Single Sign On (SSO). The GCC Network is not accessible via BYOD.

Before accessing council systems and data the application will check the version of the operating system on your device. Users should be using the latest version of the operating system; this will be technically enforced 10 days after the release date, unless there is a critical vulnerability which requires the council to enforce it sooner.

Users will have to authenticate their device using the approved council procedures in order to access any apps or data through BYOD.

4.0 Responsibilities

The **user** must accept the following:

- The BYOD system is to be used for council work only and must not be used in any way which contravenes this or any other council policy.
- Users must contact the ICT Service Desk as soon as possible if their device is lost, stolen, or otherwise compromised, to allow the council to shut down access from the personal device to council data and systems.
- Users must not allow their family members, friends or other individuals access to their personal device when it is logged into the BYOD system or any data or systems accessed through it.
- Users must not circumvent council controls, download and/or copy council data to or from their personal devices.
- Users must not screenshot, screengrab or take photos of council data on their personal devices.
- Users should ensure that any business applications provided by the BYOD system are closed before using their device for personal reasons.

- Users must be aware of their surroundings when using the BYOD system to access GCC data.
- Users should install anti-virus software on their personal device.
- A PIN/biometric lock and auto-lock timeout must be enabled on any personal device used for BYOD purposes
- Users must ensure any device used should be encrypted where this is supported, and the latest operating system is installed.
- Jailbroken (Apple) or rooted (Android) devices, i.e. devices that have had the manufacturer's built-in software restrictions removed, must not be used to access council data using the BYOD system.

The **council** will ensure that:

- Appropriate security is in place for the BYOD system to protect council systems and data.
- The tenant is configured to use an appropriate screen lock time in line with best practice.
- A user's access to council data and systems through BYOD is removed upon them leaving employment with the council.
- Activity within the BYOD environment is monitored, and any suspicious activity that breaches council policies will be investigated. Users' private activity on their personal device is not monitored.

The **council** reserves the right to:

- Revoke access to council data through BYOD where there is evidence it is not being used in accordance with this or any other council policy.
- Remove council data and any BYOD applications from the user's device – this will not affect user's personal data/applications.

The **council** will not accept any responsibility for:

- A personal device which breaks or becomes damaged whilst the user is conducted council business. It is the responsibility of the user to take out appropriate insurance, warranty agreements or repair services.
- A personal device which is lost or stolen whilst conducting business on behalf of the council.
- Any data or network charges by the network operator for the device resulting from the use of the BYOD system or access to any council data on the user's personal device.
- Any charges associated with installing and running anti-virus software the user decides to install.
- Providing technical support to a personally owned device.

5.0 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.

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

6.0 Related policies

- Code of Conduct for Employees
- Information IT Access Policy
- Data Protection Policy
- Information Security Policy
- ICT Equipment Policy
- M365 Acceptable Use Policy
- Internet and Digital Communications Policy

This policy and other related information security policies, standards and procedures can be found at Information Management and Security Policies.

7.0 Document Control

7.1 Document information

Owner:	Sherrill Holder, Assistant Director Digital and ICT
Author:	Nick Holland, Data Protection Officer
Reviewer:	IMS & DICT Policy Group
Board(s) consulted:	
Date created:	October 2022
Next review date:	April 2029
Approval:	Information Board, November 2022 (v1.0)
Date of approval:	
Scheme of delegation ref:	
Version:	1.2
Classification:	UNCLASSIFIED

7.2 Version History

Version	Version date	Summary of Changes
1.0	October 2022	First version. Approved by Information Board 16 November 2022
1.1	June 2024	Broken link fixes following launch of StaffNet on SP and replaced Email AUP with M365 AUP.
1.2	April 2026	Planned group policy review

7.3 Review

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

7.4 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