Carmarthenshire County Council

Bring Your Own Device (BYOD) Policy

Contents

1. Introduction 3
2. Bring Your Own Device (BYOD) User Agreement 4
3. Scope 4
4. Policy Statements 4
5. Usage Principles 5
6. Device Controls and Authentication 5
7. Responsibilities 6
8. Approval Process 7
9. Compliance Measurement 7
10. Custodian 8
11. Ensuring equality of treatment 8
12. Version History 8
13. Appendix 9

1. Introduction

1.1. The purpose of this policy is to allow greater flexibility to staff and elected members by allowing them to access Council resources from personal devices. This policy provides advice, guidance and mandatory measures on the use of the Bring Your Own Device (BYOD) scheme. The policy will ensure compliance with relevant legislation and best practice for the use of BYOD by ensuring that applicable and relevant security controls are set in place on all BYOD devices used to access Council information.

1.2. This policy makes references to the terms BYOD throughout and clarity on the meaning is below:

- BYOD – refers to Bring Your Own Device and is the scenario where someone chooses to use their own smartphone to access Council information and systems.

- This will allow staff to access the following Office 365 applications:
  - Your work Emails
  - Your work Teams
  - Your work Calendar
  - Your work Contacts
  - Microsoft other Office Applications

1.3. There are many benefits to the Council and its staff by allowing access to Council information from personal devices, however there are also substantial risks in that devices could be inappropriately used, lost or stolen. When using personal devices, the risks of working in an unprotected environment must be considered and mitigated where possible by use of the appropriate security systems and procedures as outlined in the policy.

1.4. It is important that staff and elected members using this scheme are fully aware of the policy and that under no circumstances should any consumer or personal ‘apps’ installed on their phones be used for work purposes. This could result in a breach of the General Data Protection Regulation (GDPR) and could result in disciplinary action being taken.

2. Bring Your Own Device (BYOD) User Agreement

2.1. All staff and elected members must accept the BYOD User Agreement, available in the appendix and shown and must be accepted during device enrolment.

3. Scope

3.1. This policy applies to any member of staff, elected member or anyone else who is using the Council's BYOD scheme. Managers also have a responsibility to ensure all staff they manage are fully aware of and understand this policy.

3.2. For the purposes of this policy, the term "Users" refers to employees, workers, contractors, agency staff and elected members authorised to participate in the Bring Your Own Device (BYOD) Scheme.

4. Policy Statements

4.1. This policy forms part of the Council's wider information governance and cyber security framework and must be read in conjunction with related Council policies. Where requirements differ between policies, the most restrictive standard applies.

4.2. The Council will implement and enforce appropriate controls and procedures on all personal devices setup to process Council information under this policy.

4.2.1. This is to ensure the Council complies with its legal obligation under the General Data Protection Regulations and Data Protection Act (2018), or any subsequent legislation to the same effect.

4.2.2. To ensure the security of Council data processed and stored within the CCC managed apps on personal devices.

4.3. This policy must be read and understood before enrolling in the BYOD scheme.

- The Cyber & Information Security Policy
- Handling Personal Information Policy and Procedure
- Breach Reporting and Response Policy
- Electronic Usage and Monitoring Policy
- Portable Device Usage Policy

4.4. Participation in the BYOD scheme is optional, and the Council will not cover any costs for using a personal device to access work systems such as email.

5. Usage Principles

5.1. Only users that have been approved by their respective Heads of Service shall be setup to use the BYOD scheme.

5.2. Only supported smartphones and tablet devices may be enrolled in Council's BYOD.

5.3. Users of the scheme that access Council information of a sensitive, confidential or Official-Sensitive nature must take all reasonable steps to protect that information from unauthorised access, disclosure, loss or viewing. Care should be taken when accessing information in public places or on shared devices.

5.4. All devices authorised will be configured to operate in line with this policy and users must sign and accept the Council BYOD 'User Agreement' before using this scheme.

5.5. Users seeking access to BYOD from locations outside the United Kingdom are required to adhere to the approval procedures detailed in Section 8 of this policy.

6. Device Controls and Authentication

6.1. By enrolling a personal device in the Council's BYOD policy, users must accept that the Council will enforce security controls and settings on the personal device, which will include, but are not limited to, the following setting:

6.1.1. Devices will not be enrolled unless they meet a minimum-security standard.

6.1.2. Biometrics such as fingerprint or face recognition can be enabled to allow access to CCC managed apps as an alternative to the PIN.

6.1.3. The device encryption settings must be enabled.

6.1.4. The number of failed logon attempts will be set to a maximum of 6 after which the corporate apps will be wiped from the device.

6.1.5. Security policies managed by Carmarthenshire County Council shall be enforced on the device to allow management of Council applications and data.

6.1.6. Users shall be required to upgrade devices and apps as soon as they are available to ensure any known vulnerabilities are patched.

7. Responsibilities

7.1. Council information must only be stored and accessed on personal devices from the approved Council managed 'apps' installed on the device.

7.2. Users must report any compromises of a BYOD device, such as being lost or stolen, to the ICT Service Desk immediately.

7.3. Any suspected or actual compromise involving a BYOD device must be reported and managed in accordance with the Breach Reporting and Response Policy.

7.4. Users are required to implement suitable measures to safeguard Council information on their personal devices. Under no circumstances should access credentials for Council-managed systems on personal devices be shared or disclosed to unauthorised persons.

7.5. When using a portable device to access Council data in public, ensure no one else can see the information on your screen (e.g., shoulder surfing).

7.6. Line managers must ensure staff have read and understood this policy and related documents, and that staff comply with it. They are also responsible for conducting risk assessments to evaluate potential policy breaches and determine if the scheme is appropriate for staff operations.

7.7. It is the responsibility of Digital Services to ensure that all managed 'apps' on a BYOD device are kept up to date. They will have no access to, and be unable to view, any personal apps or data.

7.8. Users are responsible for managing the updates for your device's operating system (such as Apple iOS updates) and ensuring it is kept up to date.

7.9. If you are travelling outside of the UK, BYOD must not be accessed and should be removed from your personal device, unless approval has been sought (see section 8).

7.10. Any access whilst outside the United Kingdom without prior approval, will result in the immediate disabling of the user account and removal of BYOD permissions.

8. Approval Process

8.1. Staff requests to use BYOD must be supported by the relevant Line Manager and approved by the appropriate Head of Service, Director or Chief Executive.

8.2. Elected member requests to use BYOD must be supported by the Democratic Services Manager and approved by the Monitoring Officer or Chief Executive.

8.3. Requests from staff to use BYOD while outside the United Kingdom must be endorsed by both a **Head of Service and a Director**, supported by a clearly articulated business need for access determined prior to departure from the UK, and will require final approval from the **Chief Executive**.

8.4. Elected members who require access to BYOD whilst outside the United Kingdom must be supported by the Democratic Services Manager and approved by the Chief Executive and Monitoring Officer.

8.5. Approvals must be time-limited and reviewed on the user's return to the UK.

8.6. Summary reports of enrolment and usage shall be made available to the Directors and Chief Executive as requested.

9. Compliance Measurement

9.1. Compliance with this policy is mandatory for staff and elected members. Breaches of this policy by staff may lead to disciplinary action being taken. Breaches by elected members may be reported to the Standards Committee.

10. Custodian

10.1. It is the responsibility of Digital Services to ensure that this policy is regularly reviewed and updated

11. Ensuring equality of treatment

11.1. This policy must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion, age, sex, gender reassignment, gender identity or expression, sexual orientation, parental or marital status.

If you require this publication in an alternative format, please contact Digital Services by emailing itsecurity@carmarthenshie.gov.uk

12.Version History

Version	Date	Actioned By	Revision Description	Approved By
BYOD Policy v1	May 2018	John M Williams	Created new Policy	Executive Board on the Oct 2018
	May 2019	John M Williams	Reviewed no changes	
	May 2020	Richard Williams	Reviewed Policy no changes	
	May 2022	Richard Williams	Reviewed Policy no changes	
	May 2023	Richard Williams	Reviewed Policy no changes	
BYOD Policy v2	19th of Oct 2026	John M Williams	Major review - policy changes to wording updated and new approval process.	Cabinet Member for Organisation & Workforce on 29th October 2026

13. Appendix

Bring Your Own Device (BYOD) User Agreement

1. Purpose

This User Agreement sets out the terms under which Carmarthenshire County Council ("the Council") permits access to Council systems and information from a personally owned device under the Bring Your Own Device (BYOD) scheme.

Participation in BYOD is **voluntary**. Users who do not wish to participate may use a Council-managed device where appropriate and available.

2. Policy Acknowledgement

By enrolling a personal device into the Council's BYOD scheme, you confirm that you have read, understood and agree to comply with the following policies, as updated from time to time:

- Bring Your Own Device (BYOD) Policy
- Cyber & Information Security Policy
- Handling Personal Information Policy and Procedure
- Breach Reporting and Response Policy
- Electronic Usage and Monitoring Policy
- Portable Device Usage Policy

Failure to comply with these policies may result in withdrawal of BYOD access and may lead to disciplinary or other formal action.

3. Ownership and Responsibility

- Your personal device remains **your property** at all times.
- All Council information accessed, stored or processed via BYOD **remains the property of the Council**.
- You are solely responsible for:

- The condition, maintenance and repair of your device
- All costs associated with the device, including hardware, insurance, repairs, tariffs, roaming, call and data charges

The Council does **not** provide technical support, maintenance or repair services for personal devices.

4. Security Controls and Device Management

By enrolling in BYOD, you understand and accept that the Council will enforce proportionate security controls on your device to protect Council information. These controls may include, but are not limited to:

- Application level management of Council approved apps
- Enforcement of device security settings (e.g. PIN, biometrics, encryption)
- Removing Council applications and data from the device where required

The Council **cannot** access or manage personal apps, content or data on your device.

5. Protective and Enforcement Actions

You acknowledge and accept that the Council may take protective actions to safeguard Council information and systems, including:

- Disabling BYOD access
- Removing Council applications and data
- Enforcing configuration or security changes
- Temporarily or permanently withdrawing BYOD permissions

These actions may be taken **without prior notice** where necessary to manage security, legal or compliance risks.

6. Loss, Theft and Security Incidents

You must report immediately to the ICT Service Desk any incident involving your device, including:

- Loss or theft
- Suspected compromise
- Unauthorised access
- Malware or security concerns

The Council may remotely remove Council applications and data as part of its incident response. You remain responsible for reporting theft to the appropriate authorities.

7. Overseas Use

BYOD access from outside the United Kingdom is **not permitted** unless explicitly approved in advance in line with the BYOD Policy.

Unauthorised overseas access may result in immediate withdrawal of BYOD access and disabling of associated accounts.

8. Data Use and Prohibited Applications

Council information must only be accessed and stored using Council-approved applications.

You must not use personal or consumer applications, cloud services or messaging platforms to store or transmit Council data, including but not limited to:

- Personal cloud storage (e.g. iCloud, Google Drive, personal OneDrive)
- Personal email or messaging services
- Social media platforms

9. Liability and Disclaimer

BYOD access is provided **"as is"**.

To the fullest extent permitted by law:

- The Council accepts **no liability** for any loss, damage, corruption, reduced functionality or data loss affecting your personal device
- This includes any impact resulting from:
    - Security controls
    - Software updates
    - Removal of Council applications or data
    - Protective or enforcement actions taken by the Council

You are strongly advised to maintain appropriate backups and insurance for your device.

10. Withdrawal from BYOD

You may withdraw from the BYOD scheme at any time. Upon withdrawal, Council applications and data will be removed from your device.

The Council may also withdraw BYOD access where required for security, compliance, operational or policy reasons.

11. Acceptance

By enrolling in the BYOD scheme, you confirm that you:

- Understand the risks associated with using a personal device for work
- Accept the responsibilities and conditions set out in this Agreement
- Consent to the enforcement of security controls as described above