Carmarthenshire County Council

Bring Your Own Device (BYOD) Policy

Contents

1. Introduction

1.1 The purpose of this policy is to allow greater flexibility to staff by allowing them to access Council resources from personal devices. This policy provides advice, guidance and mandatory measures on the use of the 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.

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 a Council employee chooses to use their own smartphone to access Council information and systems.

- This will allow you to access the following systems:
  - Your work Emails
  - Your work Calendar
  - Your work Contacts
  - Microsoft Office Applications

There are many benefits to the Council and its employees 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.

It is imperative that staff 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. Terms and Conditions

2.1 Before enrolling in the BYOD scheme, all users of the service will agree to the BYOD Scheme Terms and Conditions attached to this policy.

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.

4. Policy Statements

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

4.2 This is to ensure the Council complies with its legal obligation under the General Data Protection Regulations (2016) and Data Protection Act (2018), or any subsequent legislation to the same effect.

4.3 To promote the safe and secure use of mobile equipment, the agile working policy and improve the operations of the Council and its staff.

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

4.5 The policy will be used in accordance with the following policies, which must be read and understood before being setup to use the BYOD scheme.

- This Information Security Policy
- Handling Personal Information Policy and Procedure
- Breach Reporting and Response Policy
- Email Usage and Monitoring Policy
- Social Media Policy

4.6 Any breaches of this policy may lead to disciplinary action being taken against those who fail to comply.

4.7 This policy is approved by, and has the full support of, the Council.

5. Usage Principals

5.1 Only users that have been approved by their respective line managers shall we setup to use the BYOD scheme.

5.2 Only supported smartphones and table devices that can be managed by the Council’s BYOD may be enrolled.

5.3 All devices authorised will be configured and operate in line with this policy and users must sign and accept the Council BYOD terms and conditions before using this scheme.

5.4 The approved software for enabling BYOD by the Council is Microsoft Office 365 and this is the only system that should be used.

6. Device Controls and Authentication

6.1 By enrolling a personal device in the Council's BYOD policy, the user 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 A minimum passcode on the device of 6 numeric numbers.

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 are enabled. If not, the settings will be enforced, and the device will be encrypted.

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 we 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

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

7.1.2 Only information classed as UNCLASSIFED and OFFICIAL shall be approved for processing on a BYOD device.

7.1.3 Users must report any compromises of a BYOD devices, such as being lost or stolen, to the ICT helpdesk or Careline immediately.

7.1.4 Users must take appropriate precautions to prevent others from gaining access to Council information from their personal device. Access to Council manage systems on personal devices must never be shared or disclosed to anyone else.

7.1.5 Care must be taken to ensure that when accessing Council data using a portable device in a public place that any information displayed cannot be viewed by others. E.g. shoulder surfing (*the practice of spying on the user of an electronic device in order to obtain their personal/confidential information*)

7.1.6 Access to Council systems are not approved for use outside of the European Economic Area and users are responsible for informing ICT Services if they intend travelling outside of this area to have the access to Council information removed.

7.1.7 Line managers are responsible for ensuring staff using this scheme have read and understood this policy and all other policies referenced within. They must ensure that staff work in compliance of this policy, and are responsible for undertaking any risk assessments that may need to be carried out to understand the potential risks of staff being in breach of the policy e.g. taking into account the way staff operate, this scheme may not be suitable.

7.1.8 It is the responsibly of ICT Services to ensure that all managed ‘apps’ on a BYOD device are kept up-to-date. ICT Services will have no access to, and be unable to view, any personal apps or data.

7.1.9 You will be responsible for managing the updates for your devices operating system (such as Apple iOS updates) and ensuring it is kept up to date.

8. Compliance Measurement

8.1 Compliance with this policy is mandatory for anyone using a personal device enrolled in the Council BYOD policy. Breaches of this policy by staff may lead to disciplinary action being taken. Breaches by elected members may be reported to the Standards Committee.

9. Ensuring equality of treatment

9.1 This policy must be applied consistently to all, irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion, belief or non-belief age, sex, gender identity, sexual orientation, parental, marital or civil partnership status.

Policy approved by Executive Board:	
Policy review:	1st November 2020
Policy written by:	John M Williams (CISMP)