Portable Device Usage Policy

Contents

1. Purpose

1.1 This Policy defines accepted practices, responsibilities and procedures for the use of portable / mobile devices that the Council authorises to connect to its network.

1.2 A portable device will be defined as any electronic device that has the ability to transmit, receive, record, process or store data. This functionality is increasing in a number of devices and could have one functionality or a combination of the following functionalities:

- Laptops.
- Tablets e.g. Apple iPads, Lenovo Helix, Samsung Galaxy pads etc.
- Smartphone / Mobile Phone or Personal Digital Assistant (PDA).
- Digital recording device e.g. digital camera, audio recorded, mp3 player.
- Any other portable device, such as a satellite navigation system or a hybrid device that combines functionality.

1.3 Using personal devices to access the Council's network without prior permission from the IT Security Officer is not permitted as it poses a number of risks such as:

- Loss, disclosure or corruption of Council data on a personal device.
- Incidents involving threats to, or compromise of, the Council's IT Infrastructure (e.g. hacking, malware infection).
- Non-compliance with relevant laws and regulations such as the Data Protection Act (1998), Freedom of Information Act (2000) and the Human Rights Act (1998).
- Non-compliance with the Public Services Network (PSN) Code of Connection.
- Liability for loss of data, or damage to a personal device due to software or administrative errors.

1.4 The Authority will provide appropriate devices necessary to enable mobile working, based on receiving the relevant authorisation for the device.

1.5 This policy should be read in conjunction with the Council's Information Security Policy, Email Usage and Monitoring Policy, Internet Usage and Monitoring Policy and the Copyright Design and Patents Act Policy.

2. Scope

2.1 This policy applies to all employees, elected members and any partners or third parties who access Council data from an Authority provided mobile device.

3. Requirements & Responsibilities

3.1 The decision to provide a device for mobile working will be based on a documented business need and the request must be authorised by a Head of Service, Director or the Chief Executive.

3.2 IT Services will provide advice and guidance, based on the identified business need, to ensure that devices are compatible with our IT systems.

3.3 All devices must be procured and configured by IT Services prior to being allocated to staff for use on the Council's network.

3.4 Shared accounts will not be available on some devices (e.g. Smartphone's) due to limitations in the device software. Such devices can only be configured for single person use and cannot be shared amongst staff. E.g. Multiple mailboxes cannot be setup on iPads.

3.5 The Council expects the user to closely guard the physical security of any mobile device assigned to them that contains Council data and connects to the Council's network.

3.6 Only applications approved for business use will be installed on the Council's mobile working environment. Users are not permitted to install additional mobile "apps". This includes, but is not limited to, free apps and games from the Google Play and Apple iTunes store. On occasions, users will be asked to install updates on Apple based devices, following guidance from IT Services.

3.7 Council mobile devices will be configured to use an account for management by IT Services. This account must not be removed or modified in any way, as it could stop the device functioning correctly. E.g. Apple ID account.

3.8 Users must accept that the Council will enforce security policies on mobile devices, which are necessary to maintain the security and integrity of the data on the device. This will include, but is not limited to, areas such as passcode, passcode timeout, passcode complexity, passcode age, device encryption settings, complete wipe and device feature lockdown.

3.9 Users must immediately report loss or theft of a mobile devices to the IT Service Desk during office hours or to IT Standby (via Care Line) out of hours; this is to ensure that any Council data on the device can be remotely erased.

3.10 Users must take appropriate precautions to prevent others from obtaining access to their mobile devices. Users will be responsible for all activities made with their credentials, and should not share individually assigned passcodes or any information stored on their device.

3.11 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. entering your PIN on the device

3.12 Personal or unmanaged devices must not be used to save Council's data. This should include, but is not limited to, using personal devices with any of the Council's remote working solutions.

3.13 Public Services Network (PSN) or Government Connect Secure eXtranet (GCSX) protectively marked or classified data must never be accessed from a mobile device.

3.14 Users are not permitted to use mobile devices abroad without prior authorisation from a Head of Service, Director or the Chief Executive.. They should take into consideration the reason (business or pleasure) of the trip, additional data roaming costs which will incur for usage abroad and location of travel. Usage in regions outside of the European Economic Area (https://www.gov.uk/eu-eea) should not be permitted without seeking advice from the Data Protection Officer and IT Security Officer.

3.15 All users must ensure compliance with all relevant legislation when using a portable device e.g. Live TV should not be accessed on any Authority owned device unless you have been explicitly informed that there is a TV License in place for the premises you are currently in.

3.16 It is the responsibility of line managers to ensure devices are handed in to them prior to staff ending employment. Members should return devices to DSU. Line mangers should notify the IT Helpdesk if devices are to be reallocated or SIM contacts require termination.

4. Compliance Measurement

4.1 Compliance with this policy is mandatory for any individual who uses a portable device to connect to Council systems. Breaches of this policy by staff may lead to disciplinary action being taken. Breaches by elected members may be reported to the Standards Committee.

5. Sponsor

5.1 This Policy is owned by the Corporate Information Governance Group.

6. Custodian

6.1 It is the responsibility of the IT Security Officer to ensure that this policy is kept up to date and reviewed by the Executive Board member.

7. Ensuring equality of treatment

7.1 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.

If you require this document in an alternative format please contact the IT Security Officer on 01267 246311 or email **ITSecurity@carmarthenshire.gov.uk**

Policy written by: John M Williams CISMP