LLANTWIT FARDRE COMMUNITY COUNCIL

MOBILE DEVICE POLICY

Llantwit Fardre Community Council

Mobile Device Policy

1. Introduction
2. Definition
3. Roles and Responsibilities
4. Policy
5. Breach of Policy
6. Review

1. Introduction

1.1 Purpose

There is a greater need for Members and staff to use mobile devices whist carrying out work for the Community Council, which entails working remotely from the Council Office and occasionally at home.

The purpose of this policy is to outline Llantwit Fardre Community Council's requirements of mobile computing users in relation to the proper stewardship of mobile computing assets and the security of information accessed whilst using such devices

This policy is part of a set of Llantwit Fardre Community Council documentation covering information security and it should be read in conjunction with the:

- Data protection policy
- Data management protocol
- IT security policy
- IT acceptable use policy

The aspects of this policy relating to stewardship of Llantwit Fardre Community Council's mobile computing assets. The information security aspects of this policy apply to all mobile computing devices, both owned by Llantwit Fardre Community Council's and third-party owned devices, used to access Llantwit Fardre Community Council's systems and services remotely and on a stand-alone basis.

This policy is consistent with good practice guidance issued by **One Voice Wales** and the **Society of Local Clerks (SLCC)**

1.2 Definition

For this policy, "mobile computing devices" refer to all forms of portable computing equipment that can store digital data. Examples include, but are not limited to, laptops, netbooks, tablets and mobile phones.

1.3 Roles and Responsibilities

The Clerk is responsible for approving and regularly reviewing' Llantwit Fardre Community Council's policies which contribute to the set of documentation covering information technology and security. The Data Protection Officer is responsible for developing awareness and guidance around information security and for advising the Clerk and individual users on the use of mobile computing to meet business needs and the most appropriate technical responses to maintaining information security

Users of mobile computing devices are responsible for ensuring that such devices are purchased, used and disposed of in accordance with Community Councils policies and procedures. Users must ensure that they act in accordance with Llantwit Fardre Community Councils various information security policies and that they have completed the Councils training on information security and update training held during Llantwit Fardre Community Council's training planning sessions.

2. Policy

2.1 Stewardship of Mobile Computing Devices

All equipment purchased by Llantwit Fardre Community Council including mobile computing devices purchased by the Council remain the property of Llantwit Fardre Community Council. They must be returned to the Community Council on request or on termination of employment

Mobile computing devices should be used for the intended business need and in accordance with Llantwit Fardre Community Councils, information security and acceptable use policies, i.e. mobile devices should be used only by the Community Council' staff for company related business. Incidental personal use, allowable by HMRC, where it is consistent with any requirements of' IT policies.

The security of any institutional data stored on a mobile computing device must be given due consideration. Any unique data generated on such a device should be copied onto Llantwit Fardre data store at the earliest opportunity and interim backups stored on a secure remote hard drive, USB key or other appropriate device

Users with Accounts Software packages licenced to Llantwit Fardre Community on laptops must ensure that the software, loaded onto the machine is used in compliance with the appropriate license(s) and copyright considerations. If in any doubt, the Data Protection Officer should be consulted.

Users are responsible for maintaining the currency of the computer operating systems, antimalware and productivity applications ("patching"). Either automated (recommended) or manual method may be used. It is not permitted to make any alterations to the hardware or software that significantly impair security. If the user is not comfortable patching their device, they should return it to their IT supporter on a regular basis, allowing sufficient time for updates to be installed.

If a user has any reason to suspect that their device has become infected with malware, they should immediately cease to use it and take all necessary steps to conduct a thorough examination of the device and appropriate disinfection of the device as required.

Users should seek advice from the Data Protection Officer before passing on, discarding, or otherwise disposing of, any mobile computing device to ensure that all data pertaining to Llantwit Fardre Community Council and its Clients has been permanently deleted

2.2 Information Security

All users of mobile computing devices which access Llantwit Fardre Community Council's digital data must complete the Councils training on information security. Members and staff are required to agree to abide and adopt the policy at its Annual Meeting.

Users are responsible for the physical security of their mobile computing devices and any Members, staff or the council's client data stored on it.

Information being accessed or processed using mobile computing devices should be treated in accordance with Councils' Data Management Protocol. Any loss of mobile computing device or suspected breach of information security should be reported immediately to the Clerk and to the Data Protection Officer. Suspected theft of a mobile computing device should also be reported to police at the earliest opportunity.
Users should avoid internet café and other public wi-fi connections as these pose information security risks and should be avoided especially when accessing highly sensitive information.

Users of private devices are responsible for ensuring that they maintain anti-virus software, operating systems and security updates, as appropriate to the equipment, if they use it to access, store or process Councils Client's digital data.
Computing Services may monitor and log network and e-mail usage to protect information.

3. Breach of the policy

If a staff member or consultant is found to have acted in breach of this policy, this may lead to disciplinary action being taken against them. This disciplinary action could be up to and including dismissal.

.

4. Review of Policy

This policy shall be reviewed periodically by the Council, or sooner if changes in legislation, guidance or operational requirements necessitate revision.

Adopted by: Llantwit Fardre Community Council
Date adopted:
Review date: