COUNCIL MOBILE DEVICE POLICY

ECM DSID:	4422668
First Issued / Approved:	14 February 2023
Last Reviewed:	Date of last review C140223/7338
Next Review:	14 February 2026
Responsible Officer:	**Manager, Innovation and Technology**
Date Placed on Webpage/ Intranet:	20 February 2023

1. PREAMBLE

Mobile devices are a common and cost-effective tool for doing business. Users are also increasingly requesting the option of connecting their own mobile devices (Bring Your Own Device – BYOD) to Council equipment and networks.

1.1 Background

Council is responsible for maintaining effective security of all equipment and information within its environment.

Due to the portable nature of mobile devices, higher order security is required for these devices and for any information stored or transmitted via them.

1.2 Purpose

This policy provides direction on the deployment, use, maintenance and disposal of mobile devices within the Council.

1.3 Scope

This policy applies to the use of any Council IT infrastructure and resources by all Elected Members, staff (including work experience placements and trainees), volunteers, and consultants and contractors across Council, including Alwyndor.

Where personal devices are used to access Council information or infrastructure, this policy will apply to the extent of Council-related business.

Mobile devices covered by this policy include both Council owned devices and approved non-Council owned devices of the following types:

- notebook, laptop and tablet computer equipment
- smartphone devices used for data storage, calendars, contacts and task lists
- mobile phones where mobile internet technology is used for email correspondence
- smartphone devices capable of running third-party or downloadable applications (for example, iPhone, Android, Blackberry, Windows Mobile)
- all removable media including CD/DVD, USB devices or any other type of removable media.

1.4 Definitions

Jail break – refers to a process of removing the limitations on Apple devices running the iOS operating system through the use of software and hardware exploits.

Mobile Device Management (MDM) – refers to software that provides the following functions: software distribution, policy management, inventory management, security management and service management for smartphones and media tablets.

Rooting – refers to a process of allowing users of smartphones, tablets, and other devices running the Android mobile operating system to attain privileged control (known as "root access") within Android's subsystem.

Users refers to people using IT infrastructure and resources covered by this policy, namely Elected Members, staff, volunteers, consultants and contractors.

1.5 Strategic Reference

The innovation focus area includes aspirations of creating conditions for early adoption and experimentation with beneficial technologies and using digital tools to create transparency and enable direct participation.

2. PRINCIPLES

2.1 Council embraces the value that IT infrastructure and resources can add to the workplace and will provide all relevant users with appropriate tools to undertake their work effectively.

2.2 All mobile device use must comply with the Acceptable Use Policy. Additionally, mobile devices are subject to the following:

- only mobile devices owned and operated by Council may be used to connect to Council's infrastructure or services without obtaining prior approval from the Manager IT
- any installed management software, such as mobile device management and anti-virus software, must not be removed and must be kept up to date as directed by IT
- Council owned mobile devices remain the property of Council, unless they are disposed of in line with asset disposal schedules
- USB sticks from an unknown or un-trusted source are not to be connected to Council equipment
- Council owned devices are locked Council's chosen network provider
- users are responsible for ensuring mobile devices are not accessed by unauthorised persons
- users may be held responsible for damage to mobile devices if they do not take due care
- to prevent opportunistic theft, mobile devices must never be left unattended in a public place, in unsecured conditions or visible in vehicles. Where possible, devices should be securely locked away, or

special cable locking devices should be used to secure the equipment to a non-removable fixture

- mobile devices should be carried as hand luggage when travelling by aircraft
- every reasonable effort should be made to ensure that Council information is not compromised through the use of mobile equipment in public places. Screens displaying sensitive or critical information should not be seen by unauthorised persons.

2.3 At the end of a mobile devices useful life, it is to be provided to IT who will ensure it is disposed of in a manner that maximises the potential for reuse or recycling with minimal associated environmental impact.

2.4 In some circumstances, users may be permitted to connect non-Council owned mobile devices to Council systems and infrastructure for the purpose of multi factor authentication, receiving email, contact and calendar information and remote desktop access. Permission must be granted by the Manager IT.

2.5 Where a non-Council owned mobile device is connected to Council systems, users accept the following conditions:

- installation of the City of Holdfast Bay mobile device management (MDM) on the device, which will enforce:
  - a timer lock with a mandatory, unique and instantly changeable 6 digit passcode
  - after 6 failed login attempts, all Council data and settings will be automatically deleted
  - limits to the number of days of corporate mail and calendar items stored on the device
  - enables remote selective wipe of all Council data.
- users will notify IT immediately upon loss, theft or suspected loss/theft of the device to enable data to be remotely erased and services disabled
- users agree to protect Council information from unauthorised use
- non-Council owned devices will not be supported by IT with the exception of connectivity to Council services
- Council is not responsible for the functionality, serviceability or performance associated with non Council-owned devices, and accepts no responsibility for communication charges incurred while performing Council business
- Council accepts no responsibility for loss of data from non-Council owned devices, or any loss or damage of the device
- device operating systems must be kept up to date and users agree to not jail break or perform rooting of their device.

3. REFERENCES

3.1 Legislation

Local Government Act 1999
State Records Act 1997

3.2 Other References

Information Security Policy
Social Media Policy
Acceptable Use Policy
Elected Member Code of Conduct
Employee Code of Conduct
AS ISO/IEC 27001:2015
AS ISO/IEC 27002:2015
Fair Treatment Procedures
Managing Misconduct & Disciplinary Procedures
Workplace Relations Policy
Quality Working Culture Policy