Mobile Device Policy

Policy Endorsement:	Endorsement Required by Executive Team		
Policy Superseded by this Policy:	Not Applicable		
Directorate:	Digital Technology		
Responsible Officer:	Chief Information Officer		
Policy Type:	Discretional		
File Number:	A4361867	Version No:	4
1st Adopted by EMT	October 2012	Last Adopted by EMT:	19 February 2025
Review Period:	4 years	Next Review:	February 2029

This page has been left intentionally blank.

TABLE OF CONTENTS

1. POLICY OBJECTIVE (OR PURPOSE)

To provide a framework for the effective and efficient use of mobile devices such as smartphones and tablets, to assist with effective communication, provide appropriate security, increase operational efficiency and enhance Council's responsiveness and delivery of services to the community.
This includes dealing with Council property in particular in relation to device management, security and privacy.
To provide clear guidelines on what activities are permitted and what activities are restricted thereby ensuring that processes regarding mobile devices assist communication related to Council's business in flexible and cost effective manner.
The objectives of this policy are compatible with the Charter of Human Rights and Responsibilities Act 2006.

2. BACKGROUND

The Mobile Device Policy was developed to address the increasing use of mobile devices such as smartphones and tablets within the organisation. The policy aims to provide a framework for the effective and efficient use of these devices to enhance communication, ensure security, increase operational efficiency, and improve the Council's responsiveness and service delivery to the community.

3. SCOPE

This policy applies to all Council employees regardless of status or position, Workplace Participants (persons not engaged directly by Council including contractors, agency staff, and volunteers – e.g. 'engagement' through external providers), Councillors and any other parties who are issued with a Council owned mobile device. Hereafter all person covered by this policy are referred to as 'users'.
This policy applies to all Council owned mobile devices that have access to Council networks, data and information systems, excluding laptops. Laptops are dealt with under the Information Security Policy.
This policy should be read in conjunction with *Staff Code of Conduct* (as applicable)*, Councillor Code of Conduct* (as applicable), *Electronic Media Policy, Social Media Policy* and the *Information Security Policy*.

4. DEFINITIONS

Mobile Device - Mobile device is a generic term used to refer to a small, portable electronic device that can be carried around and used without an external power supply such as a smartphones or tablets

Digital Technology - the Council's department providing Information Technology Services.

Jail-broken - to jail-break a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all features and enabling the installation of unauthorised software.

Mobile Device Management (MDM) - software that manages Council's Mobile Devices.

Malware - Malware is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems or display unwanted advertising.

Internet Service Provider (ISP) - an organisation that provides services for accessing the Internet.

5. POLICY

Potential users who are deemed to meet one or more of the requirements set out below, upon written request to the Digital Technology Service Desk from the Manager of the Business Unit, will be provided with a mobile device:

- Demonstrated business need [i.e. necessary to their position];
- Safety and security of staff;
- Requirement to perform after hours duty;

Please note that Council reserves the right to issue and withdraw the use of Council issued mobile devices at its discretion. This includes but is not limited to access to Council software programs and calendar / email systems.

Appropriate Use

Connection / Restricted Phone Numbers

Council issued mobile devices must only be connected to Council preferred service providers, on an approved corporate voice call/data plan. Users are reminded not to access 'pay-for-time' telephone numbers unless these are directly related to their work. Overseas roaming for international calls will NOT be enabled.

Global Roaming

Due to State Government direction, Global Roaming will not be enabled for Council mobile devices and the devices cannot be taken overseas.

Personal Use

Mobile devices have been issued for business purposes; therefore private usage should be limited. Reasonable personal use of Council provided mobile devices is permitted in recognition of the fact that users may at times need to make personal calls as a result of work demands or incidental matters.

In some cases the person may be asked to reimburse Council for personal use and/or return the device.

Security

Mobile devices must not be shared as they store personal and Council information, e.g. emails, calendar and contact information. Users are responsible at all times for managing Council and personal data stored on the device. All reasonable precautions must be taken by users to protect the privacy and confidentiality of Council information stored on the device at all times. This includes preventing others from accessing or using the device in a manner that enables them to obtain Council information to which they would not normally have access. Users must take all reasonable care to ensure mobile devices are safely secured at all times to prevent damage, loss, theft or access by unauthorised persons. Additionally, users are expected to apply security updates to their device to address security vulnerabilities (failure to update may trigger corporate applications to stop working until security patches are applied).

Wi-Fi

Mobile devices are equipped with Wi-Fi connectivity which by default will be turned on. When the device is in range of Council's Wi-Fi infrastructure, the device will automatically search and connect to the preconfigured Wi-Fi option. When mobile devices come within range of Council's Wi-Fi infrastructure they must be allowed to connect to these systems. Users are required to take care if they use non-CGD Wi-Fi connections at any time as these services are not supported by DT.

Use of Mobiles Devices in Vehicles

Under Victorian law, the use of mobile devices while driving is prohibited unless an approved hands-free device or integrated vehicle system connection is used. Accordingly, Council issued mobile devices must only be operated in this manner while driving. Penalties incurred for failing to comply with the law will be the driver's personal responsibility.

Device Procurement, Management and Security

Device Procurement

Procurement of additional mobile devices with SIM cards requires the approval of relevant Managers. Users needing a mobile device may port over their existing phone number to the Council service provider with written approval from their Manager. Any fees incurred during this process will be charged to that user. The mobile device will remain the property of the Council at all times.
Lifespan of mobile devices is typically between 2-3 years. From 2025/26 FY the replacement of devices, including cost, is the responsibility of the Digital Technology department. At this time or at cessation of employment or engagement the user must return all mobile devices, any associated equipment and accessories to the Digital Technology department.

Device Management

Users will be given assistance by DT to create a corporate iTunes / Google Play account (utilising a council email address) necessary to activate and manage their mobile devices. In the event that users do not have a corporate email address they may use a personal email address for this purpose.

Corporate iTunes / Google Play accounts must be established for users who are required to utilise any corporate *'volume licencing'* software applications for their roles with Council. Council uses a Mobile Device Management (MDM) system to manage mobile devices. The MDM application must not knowingly be turned off when the device is powered on.
DT will support approved hardware and software, but is not accountable for conflicts or problems caused by the use of unapproved, hardware, software or peripherals such as car Bluetooth connections. In these cases DT will not provide support.
Council reserves the right to block users from installing specific applications which have compatibility issues with Council installed software, or which are deemed to be inappropriate by the Department Manager in consultation with DT.
Devices must:

a) not be "jail-broken" or have any software installed which is designed to gain access to functionality not intended to be exposed to the user.
b) be kept up to date with manufacturer or network provided operating software updates; accordingly users must regularly check for and install updates.

Council reserves the right to delete all corporate information from the device if requested by the relevant manager and approved by People and Change.

Security of Mobile Devices

Council will regularly collect information regarding the mobile device, including but not limited to version information, installed applications, call details, amount and frequency of data downloaded and location information. Please refer also to the section of this policy titled Information Privacy and Data Information.
Users must follow Council's *Information Security Policy* in regard to using passwords, PINs and/or encryption on all Council issued mobile devices. This is in addition to the reasonable physical security measures outlined in the Security section above.
DT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed a breach of the Appropriate Use section of this policy and will be dealt with in accordance with Council's *Information Security Policy*. Council may also need to track the location of a mobile device if it has been reported lost or stolen.
In the event that a mobile device is damaged, lost or stolen users must contact the DT Service Desk immediately, and then contact their manager and the Risk Management Coordinator as soon as possible, so that all necessary steps to protect the privacy of the Council data are carried out without delay.

DT will immediately arrange for a bar to be put on the mobile device so that it is not able to be used and wipe all corporate data from that mobile device to the extent possible. The intention is that no personal data will be affected; however it is possible that personal data will be removed from the mobile device during this process and Council takes no responsibility for the loss of such data.

Information Privacy and Data Information

Collection of call and Data Information

When using a Council owned mobile device, Council will collect detailed information for billing purposes regarding use of the device, including but not limited to details regarding the dates, times, locations and types of calls made and in some cases received, messages or data sessions as well as information about the associated phone numbers or metadata. Council will use this information primarily for billing purposes; however, Council reserves the right to use this information for secondary purposes such as monitoring compliance with legal requirements and Council policies. Managers will handle this information with regard to obligations under Council's *Privacy and Personal Information Policy*.

When using a Council owned mobile device additional information regarding the device and its activity may also be collected and used by Council for billing purposes and in order to monitor compliance with this and other Council policies.

Collected information may include:

- Operating system and applications installed and used;
- Location information;
- Phone call history;
- Internet browser history;
- Council emails sent and received;
- any other information required by Council.

6. RESPONSIBILITIES

1. Department Manager

Mobile Device Order / Authorisation

Department Managers will assess which potential users need to be provided with a mobile device as determined by the parameters set out in the Eligibility section above. All new or replacement mobile devices will only be issued once this has been determined by the relevant department manager. Once determined the relevant manager will send written authorisation to the DT Service Desk detailing the debiting account number. Managers must also approve the cost of any licences necessary to manage a mobile device connected to the corporate network and this cost will be allocated to the relevant department.

Mobile devices issued for use will be standard / base models, as determined by the Chief information officer. Non-standard devices will not be provided to users unless prior approval is given by the relevant Director through a detailed business case having being submitted. All mobile devices must be purchased through DT.

Mobile Device Use / Monitoring

Managers are responsible for monitoring the use of Council owned mobile devices by users in their department.

Transfers or disconnections of service

Managers must notify the DT Service Desk with details of any transfer of mobile devices between users and any suspensions or cancellations of mobile numbers. To disconnect a mobile device, the department manager must notify the DT Service Desk, by including in the request (a) the device number and (b) the name of the person to whom the mobile device had been issued to ensure that the correct device has been identified

Managers must collect all Council owned mobile devices from users at the cessation of their employment or engagement with Council and return the devices to DT for decommissioning or reissue to other Council officers or departments. If the device is still required by the department, it may be reissued by DT.

Managers are responsible for notifying the DT Service Desk of the cessation of employment or engagement of users with Council for the purposes of disabling access to Council systems and/or deletion of corporate information.

2. Digital Technology (DT)

Mobile Device Purchase, Register and Billing Information

DT will arrange the purchase of all mobile devices upon receipt of authorisation by the relevant manager. DT will debit the cost of all purchases and repairs to the appropriate sub activities of relevant departments. DT will also maintain a Mobile Device Register to ensure utilisation of mobile devices is consistent across Council. Monthly mobile device accounts are made available to employees. Managers can view this information through the billing system. DT Service Desk will advise when this data is available.

Repairs

If a mobile device requires repair, the user is to alert the relevant department manager and then contact DT immediately. For devices still under warranty, the user may be directed by the DT Service Desk to make an appointment and attend at the nearest Authorised Service Centre. Any costs incurred for repairs to mobile devices not covered by warranty will be charged to the relevant department. Users are responsible for timely repair of device.

Loss / Theft, or Transfer / Disconnection of Service

Upon determination that a mobile device is damaged beyond repair, lost or stolen, relevant department managers may submit an email or ticket request to DT for a replacement mobile device (if one is available) DT will arrange the purchase of a new mobile device including, where appropriate, a replacement SIM card with the same phone number as allocated to the previous device. For transfer or disconnection of a mobile device, see Transfers or disconnections of service section above.

7. REPORTING, MONITORING AND REVIEW

To ensure the standards of this policy are met, Digital Technology will measure, conduct regular audits and assessments and monitor compliance with security protocols and identify potential vulnerabilities. Incident reporting mechanisms will be established, enabling staff to promptly report security breaches or suspicious activities. The success of the policy will be reviewed through periodic evaluations, including analysis of incident reports, audit findings, and feedback from users.

8. REFERENCES AND RELATED DOCUMENTS

Related Council and Other Policies, Procedures, Strategies, Protocols, Guidelines

- Code of Conduct - Staff
- Code of Conduct – Councillor
- Councillor Support and Reimbursement Policy
- Privacy and Personal Information Policy
- Information Security Policy
- Policy for Performance Management and Behavioural Issues
- Procurement Policy
- Records Management Policy
- Social Media Policy
- *Privacy and Data Protection Act 2014*