EMPLOYEE MOBILE DEVICE POLICY

Approval Level:	EMT
Policy Type:	Organisation
Approval Date:	14/12/2021
Review cycle:	Four years
Review Date:	15/12/2025
Responsible Officer:	Manager Information Technology
Owner:	Information Management
Responsible Director:	Corporate Performance
Relevant Legislation/Authority:	*Privacy and Data Protection Act 2014* *Freedom of Information Act 1982* *Charter of Human Rights and Responsibilities Act 2006*
DOCSETID:	3482760

1. PURPOSE

The purpose of this policy is to:

1.1 Support effective and efficient care and use of Mobile Devices and minimise disruptions to services and activities;

1.2 Ensure that the use of Mobile Devices and BYOP complies with the City of Greater Bendigo's (the City) Code of Conduct and procedures, applicable policies and laws;

1.3 Ensure that the use of Mobile Devices and BYOP is consistent with the City's business operations and organisational objectives and;

1.4 Ensure that Authorised Users understand their obligations and accountability when using Mobile Devices or BYOP.

2. SCOPE

This policy applies to all Authorised Users. The option to BYOP is only applicable to Employees of the City and excludes volunteers, councillors, students and contractors.

3. DEFINITIONS

In this policy:

Authorised Users means Employees, volunteers, students, trainees, apprentices and contractors who use City Applications to perform City Functions.

Bring your own Phone (BYOP) means an Authorised User using their Personal Phone to perform City Functions.

City means The City of Greater Bendigo.

City Applications means the software systems used to support City Functions.

City Functions means the activities undertaken by an Authorised User to meet organisational objectives.

Email means electronic mail which is the transmission of messages over communication networks.

Employee means a person who receives a salary or wages from the City (employed on either a full-time, part-time or casual basis where the nature of the work is permanent/ongoing or temporary for a specified period).

Encryption means the process of converting data to an unrecognisable or "encrypted" form. It is commonly used to protect sensitive information so that only authorised parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the internet.

Mobile Device Management (MDM) means security software used to monitor, manage and secure mobile devices.

Mobile Device means a device that is used in a portable fashion that includes mobile phones, smart phones, tablets and laptops/notebooks. For the purpose of this policy, this refers to Mobile Devices that are supplied by the City.

Personal Phone as per BYOP, means a mobile phone that has not been supplied by the City.

Portable Storage Devices (PSDs) means any type of storage device that can be removed from a computer. Examples include portable hard drives, USB keys, memory cards CDs and DVDs.

4. POLICY

The City commits to supporting Authorised Users and the efficiency of service delivery available through the use of Mobile Devices and BYOP. This policy establishes reasonable

controls over the allocation and use of Mobile Devices and BYOP to ensure appropriate use and adequate resourcing.

4.1 Mobile Devices

(a) Authorised Users are responsible for ensuring Mobile Devices are used and stored in a way that they are not prone to theft, misuse, extremes of heat and cold, moisture and other environments where they may be subject to physical damage.

(b) Authorised Users are responsible for ensuring that all Mobile Device accessories such as power supplies and mice are not misplaced or lost.

4.1.1 Mobile Device Models and Accessories

(a) In consultation with the appropriate business unit, Information Management will determine the appropriate make and model Mobile Device that will fully support an Employee's work duties. Relevant business units will be charged for the device, any accessories and any maintenance of the device required.

(b) Employees are responsible taking all reasonable measures to prevent the loss of mobile devices and accessories such as carry cases, power supplies and mice. In consultation with the relevant business Unit Manager, Employees may be charged for replacing the items.

4.1.2 Personal Use

The City allows limited personal use of Mobile Devices under the following circumstances:

- the purposes are personal and private;
- there is no financial gain;
- it does not interfere with the City's operations;
- there are no unreasonable or excessive charges;
- all policies are complied with and;
- the device and corporate information is not significantly exposed to loss, theft or damage.

4.1.3 Costs and Charges

Costs and charges for all Mobile Devices will be charged to the relevant business unit. All Mobile Device related expenditure is monitored. Authorised Users may be asked to identify private costs at the request of Unit Managers and submit details to Information Management for invoicing.

4.2 Bring Your Own Phone (BYOP)

(a) Where BYOP is determined as required to support City Functions, BYOP will be implemented on a case by case basis by agreement between Information Management, the Authorised User and their unit Manager or Director as relevant.

(b) Eligibility for BYOP will be determined based on a number of considerations, including but not exclusively;

- whether out of business hours contact is an expectation of the role
- whether field work is part of the role
- whether customer contact from outside the office buildings is required as part of the role
- the need for receiving calls, making calls or both
- the need for internet access is part of the role
- whether existing Council mobile devices are allocated or available to the role.

(c) A requirement of BYOP is that MDM is installed on the device.

(d) Information Management may decline or revoke a BYOP request if the device is deemed to be non-secure.

(e) The City supports BYOP where the Authorised User supplies both the device and the associated data plan. No alternative BYOP arrangements will be considered.

(f) All costs associated with the purchase and use of BYOP remains at the expense of the Authorised User.

(g) The City will assist in setting up City Applications. Any costs associated with City Applications, MDM or remote management tools will be paid for by the City. Support from Information Management will not be provided for non-City Applications.

(h) Where it is reasonably expected that the personal phone number of the owner of a BYOP will need to be used for communication within the context of an Authorised User's assigned responsibilities, the Authorised User's personal mobile phone number may be published on the intranet, in corporate staff directories, Email signature or websites as required.

(i) It is the Authorised User's responsibility to request any updates or setting up of additional City Applications from Information Management as required.

(j) BYOP eligibility will be reassessed periodically. When there is no longer a requirement to use a BYOP to support City Functions, the device must be presented to Information Management for the removal of City Applications.

(k) Staff with an approved BYOP arrangement are eligible to receive a fortnightly BYOP allowance as detailed in Appendix A.

4.3 Security

(a) It is the Authorised User's responsibility to know the location and ensure the security and appropriate use of the Mobile Device at all times.

(b) While the City supports a mobile and flexible workforce, there are a number of inherent risks involved in working away from a standard office environment. When Mobile devices and BYOP are connected to the City's network (i.e. when working in the office), they have a greater level of protection from threats via a number of corporate security tools.

(c) There is an expectation that Authorised Users who work remotely will need to periodically attend the office personally and bring their Mobile Device or BYOP for security updates, maintenance and support of City Applications. This will be at the request of Information Management as required.

(d) If a Mobile Device or BYOP is lost or stolen, the Authorised User must report it to the appropriate Manager/Director and Information Management as soon as practically possible. Information Management will attempt to remotely locate the Mobile Device or Personal Phone via GPS. If the Mobile Device or Personal Phone is believed to be stolen, that it may be misused or that corporate information is at risk, then Information Management may at its discretion attempt to remotely lock and or wipe the device. This will likely result in the loss of any personal information stored on the Mobile Device or Personal Phone.

(e) The storage of corporate documents and information on Mobile Devices and Personal Phones will increase the need to remotely wipe the Mobile Devices or Personal Phone if lost or stolen. For this reason it is crucial that Authorised Users store and manage documents and information according to the appropriate City Applications and relevant expectations.

4.4 Faulty / Damaged Equipment

(a) If a Mobile Device is faulty or damaged, the Authorised User is to notify Information Management as soon as possible. Information Management will then determine an appropriate solution to rectify the fault or damage.

(b) Relevant business units may be charged for any repairs of Mobile Devices. In consultation with the relevant business unit Manager, Authorised Users may be charged for the repair.

(c) With the exception of maintaining City Applications, the City is not responsible for the maintenance and repairs of Personal Phones, even if the fault or damage occurred while it was being used for City Functions. If a Personal Phone is lost or fails it is expected that a replacement device will be sourced or alternate arrangements are put in place by the Authorised User.

4.5 International Roaming

(a) Approval is required by the relevant Manager/Director prior to taking a Mobile Device overseas.

4.6 Voicemail

(a) Voicemail messages on Mobile Devices and Personal Phones must be setup and recorded in line with Corporate Guidelines

(b) Voicemail messages are considered a customer request. All voicemail messages must be responded to in line with the expectations described in the Customer Service Charter.

4.7 Portable Storage Devices (PSD)

(a) PSDs will be issued to Authorised Users with demonstrated business needs which cannot be met by using other more secure processes. PSD's will be registered with a unique number and assigned to an Authorised User. Information Management will install necessary security controls on to the PSDs and these are not to be removed or circumvented. Approved PSD's are the only PSD authorised to store City information

(b) All PSDs used to support or perform City functions must be encrypted.

(c) Unencrypted PSDs will be restricted to read only on all City devices.

(d) All PSDs must be kept secure by the Authorised User responsible for them.

(e) Information Management will adequately train Authorised Users to operate the PSD upon issuing the PSD.

(f) Authorised Users are responsible for the secure storage, transmission, access and disposal of information contained in PSDs. Authorised Users must take necessary care from unauthorised use, destruction and theft of PSDs and the data they contain. Authorised Users must notify Information Management as soon as possible following an incident which may lead to loss or theft of corporate information. All PSD's are to be returned to Information Management when they are no longer required for business needs or prior to the assigned Authorised User's relationship with the City ceasing.

4.8 Acceptable Use

In addition to the expectations described in this policy, the use of Mobile Devices, BYOP and PSDs must adhere to:

- all road rules;
- the City's Employee Code of Conduct;
- all other relevant City policies and procedures and;
- all relevant legislation

5. ROLES AND RESPONSIBILITIES

5.1 Authorised Users

All Authorised Users are responsible for:

(a) Reporting lost or stolen Mobile Devices and PSDs to Information Management and their Unit Manager/Director as soon as practically possible;

(b) Maintaining a secure and complex pin code, facial recognition or fingerprint to prevent unauthorised access;

(c) Ensuring device inactivity locking is enabled;

(d) Presenting the Mobile Device or BYOP to the office for account creation and management, maintenance and/or support as required and requested by Information Management;

(e) Ensuring that Mobile Devices and Personal Phones are kept up to date with the latest available software and application updates;

(f) Regularly familiarising themselves with security advice as per The Information Management section of SharePoint. https://cityofgreaterbendigo.sharepoint.com/sites/InformationTechnology/SitePages/Avoiding-Phishing.aspx.

Excluding BYOP, all Authorised Users are responsible for:

(g) Proper care, maintenance and use of the Mobile Device and PSD;

(h) Ensuring that the running costs associated with the Mobile Device are kept to a minimum.

5.2 Information Management

Information Management is responsible for:

(a) Authorising the purchase of all Mobile Devices and network connection setup;

(b) Authorising PSD purchases;

(c) Maintenance and service of Mobile Devices;

(d) Enabling international roaming;

(e) Coordination and delivery of relevant training of Mobile Devices and PSDs to Authorised Users;

(f) Recording Mobile Devices and PSDs on the asset register;

(g) Allocation of phone numbers to Authorised Users with authorised data or voice plans;

(h) Distribution of usage reports to the appropriate Manager/ Director;

(i) Installation and management of City Applications, MDM tools and anti virus software on Mobile Devices and Personal Phones;

(j) Maintenance of billing system and provision of call cost information to Financial Strategy;

(k) Monitoring of data and call usage and;

(l) Invoicing to Individuals of costs associated with private use at the discretion of the appropriate Unit Manager/Director.

5.3 Unit Managers / Directors

Unit Managers (or Directors as appropriate) are responsible for:

(a) Approval of all device purchases to meet the requirements of an individual's role;

(b) Approving BYOP in consultation with Information Management and the Authorised User.

5.4 People Managers

People Managers are responsible for:

(a) Approval of repairs as advised by Information Management;

(b) Budgeting for the acquisition, maintenance, replacement of Mobile Devices and all related expenses relating to the unit and;

6. RELATED DOCUMENTS

Employees are encouraged to access the related internal documents which are available on the intranet and/or external resources which are available as per the below.

These include:

- Appropriate Workplace Behaviour Policy (DOCSETID 1822685)
- Customer Service Charter (DOCSETID ID 4051596)
- City of Greater Bendigo Code of Conduct (DOCSETID 3603208)
- Flexibility at Work Policy (DOCSETID 4416636)
- General IT Use Policy (DOCSETID 1739680)
- Managing Misconduct Procedure (DOCSETID 2172947)
- Prevention of Sexual Harassment in the Workplace Policy (DOCSETID 4579152)
- Social Media Policy (DOCSETID 1863281)
- Mobile Device Procedure (DOCSETID 4599922)
- Privacy Policy (DOCSETID 4322695)
- Bring your own Phone Agreement

Further information or advice on this policy should be directed to Information Management

7. HUMAN RIGHTS COMPATIBILITY

The implications of this policy have been assessed in accordance with the requirements of the Victorian Charter of Human Rights and Responsibilities.

8. ADMINISTRATIVE UPDATES

It is recognised that, from time to time, circumstances may change leading to the need for minor administrative changes to this document. Where an update does not materially alter this, such a change may be made administratively. Examples include a change to the name of a Business Unit, a change to the name of a Federal or State Government department, and a minor update to legislation which does not have a material impact. However, any change or update which materially alters this document must be made through consultation with the staff Consultative Committee and with the approval of EMT or where required, resolution of Council.

9. DOCUMENT HISTORY

Date Approved	Responsible Officer	Unit	Change Type	Version	Next Review Date
November, 2021	*DS*	*Information Management*	*Reviewing Employee Mobile Device Policy and*	*3*	*November, 2025*

			incorporating Portable Storage Device Policy		
December, 2021	*DS*	*Information Management*	*Updated incorporating EMT feedback*	*4*	*December, 2025*
Dec 2021	*RM*	*Governance*	*Admin following approval*	*5*	*December 2025*

Appendix A.

Where a BYOP agreement has been entered into by agreement between Information Management, the Authorised User and their Unit Manager or Director as relevant and the Authorised User has signed the associated Bring your own Phone Agreement, they will be entitled to a fortnightly allowance. This allowance will be $25 for full time staff. For staff who work less than 76 hours per fortnight the allowance will be calculated on a pro rata basis with a minimum payment of $5 per fortnight.