

# Mobile Device Management (MDM) on a Personal Smartphone

<b>Policy Type: Operational Policy</b> <b>Policy Owner: ICT Manager</b>	<b>Policy No.: OP-038</b> <b>Last Review Date : 5 August 2020</b>
--	--

The City of Melville (CoM) acknowledges the use of mobile phones by staff as a tool to support work related activities.

Two options are available to applicable employees:

1. Bring Your Own Device (BYOD) - Staff will use their personal mobile phone device in order to access the work environment. The mobile phone device is subject to approval by the City. An allowance may be provided by the City to support the BYOD option.
2. Work Provided Device - The City will provide applicable employees with a mobile phone device. Restrictions around the use of this device will apply.

## Policy Objectives

The objective of this policy is to provide details on the City's approach to the work related use of mobile phones in compliance with the Policy scope.

## Policy Scope

This policy applies to approved employees only and specifically excludes Contractors and Volunteers.

CoM reserves the right to revoke this privilege or apply other disciplinary processes if users do not abide by the policy outlined below.

## Definitions

- Acceptable Business Use - Activities that directly or indirectly support the business of CoM.
- Jailbroken - Where the restrictions have been bypassed on an Apple device to take full control of the device e.g.to install unauthorised apps or to remove the security protections.
- Mobile Device Management (MDM) - An industry term for the administration of mobile devices, such as smartphones, tablet computers and laptops.
- Rooted - A device with restrictions removed to allow access to low-level functions. It often refers to an Android device.
- Smartphone - A mobile device with telephone and computer capability.

## Policy Statement

### General

1. Access to work related information will be via the City's MDM tool only.
2. The mobile telephone number associated with a BYOD shall be made available for internal City business use.

### Devices and Support

1. Work related messages and photographs are to be recorded into ECM as per City protocols.
2. Approved employees are responsible for maintaining their own device.
3. Approved employees are responsible for maintaining all applications and information on their device outside of the MDM environment.
4. ICT Services is responsible for setting up the work related controls and removing them.
5. The employee is responsible for selecting a suitable data and voice plan to support both their personal and work required usage requirements.

### Security

1. Any work related activity undertaken on a mobile device shall be within the MDM environment and in accordance with the Code of Conduct and other reasonable instructions provided by the CoM for employees.
2. Access to the MDM environment is password protected for use by approved employees only.
3. Lost or stolen devices must be reported to ICT Services as soon as possible (ideally within 48 hours).
4. The CoM reserves the right (the employee will be notified) to remove the MDM tool if:
  - a. the device is reported as lost or stolen; or
  - b. the employee ceases employment with the City (after close of business of the day the termination takes effect); or
  - c. ICT Services detects a data or policy breach, a virus or similar threat to the security of the City's data and information infrastructure.
5. Any communication allowance will be reviewed and may cease in relation to non-compliance of this Policy and for lost or stolen devices until the MDM is re-installed.
6. Subject to review, the City reserves the right to provide a Loan device with access to the work environment for a maximum of thirty (30) days post the inoperable personal smartphone with the CoM's MDM installed, unless otherwise approved by ICT Services. As a CoM device other limitations may apply and the device type will be selected as to best meet CoM requirements.

### Allowance Paid for a BYOD

1. A prescribed allowance (as updated) currently \$25.00 per fortnight will be paid to approved employees and is a payment to acknowledge the City's access to a personally owned smartphone for use on CoM business.
2. Eligibility criteria includes:
  - a. The use of a smartphone has been identified as an inherent requirement for an employee to perform their work (linked to Position Description);
  - b. Employee who is being paid higher duties to fill a position that has been identified as requiring a smartphone;
  - c. Approval has been provided by an employee's Supervisor to require access on a temporary basis for a special purpose;

- d. The employee has a personal smartphone that operates using an iOS or Android operating system;
  - e. The employee has a personal smartphone that supports the apps needed for the employees' position;
  - f. The smartphone the MDM is to be installed on does not have a Rooted (Android) or Jailbroken (iOS) operating system.
3. The allowance will commence once the MDM has been accepted on the personal device.
  4. The requirement for this allowance is effective for 12 months (excluding ELT and MLT which is for the duration of the employment contract) and further allowance is subject to review unless an alternate agreement is in place.
  5. The City may reimburse for additional work-related communication charges above the allowance subject to approval

### **Risks/Liabilities/Disclaimers**

1. While ICT Services will take every precaution to prevent the employee's personal data from being lost in the event it must remotely wipe a device, it is the employee's responsibility to take additional precautions in terms of backing up personal data such as emails, photos, contacts, etc. The CoM takes no responsibility for availability or protection of personal data on the personal smartphone.
2. The employee is expected to use the MDM app in an ethical manner at all times and adhere to the City's Code of Conduct.
3. CoM reserves the right to take appropriate disciplinary action inclusive of a review of employment including termination for non-compliance with this policy.
4. The employee is to ensure the operating system is kept updated.
5. The employee must take reasonable steps to ensure the security of the MDM environment.
6. All employees who have a registered personal mobile device for business use acknowledge that the CoM owns all intellectual property created via the MDM;
7. Provision of a phone or an allowance does not place an individual on call (unless advised) which means you do not have to respond to work requests outside of the ordinary span of work hours (unless on overtime)

### **Other References that may be applicable to this Policy**

Legislative Requirements:

Delegated Authority:

Plan / Policy / Framework:

- IT Security Policy
- Recordkeeping Policy
- Code of Conduct

Procedure:

- IT Security System Procedure

Work Instructions / Process Maps:

Forms / Supporting Documents (internal):

- Application for SmartPhone Access to COM Related Information
- Request an App for a Mobile Device

Supporting Documents (external):

---

### **Origin/Authority**

ELT Meeting

18 December 2019

### **Reviews**

5/8/20 – Accepted by MLT and ELT

- BYOD allowance rate changed from \$13.46 to \$25.00 per fortnight
- Reference to supporting forms