

Victoria Police Manual – Procedures and Guidelines

Mobile / Smart Phones

Source Policy

These Procedures and Guidelines support and must be read in conjunction with the following:

- VPMP IT equipment and software

The following references provide additional information or requirements of relevance:

- VPMP Appropriate use of information
- VPM Recording devices, CCTV and digital asset management
- VPMG Portable computing devices
- VPMP Information use, handling and storage
- VPMP Information review, retention and disposal

Application

Procedures and Guidelines are provided to support the interpretation and application of rules and responsibilities. They include recommended good practices and assessment tools to help employees make lawful, ethical and professional decisions. Employees should use the **Professional and ethical standards** to inform the decisions they make to support interpretation of Procedures and Guidelines.

Procedures and Guidelines are not mandatory requirements on their own. However, where rules and responsibilities state that employees must have regard to Procedures and Guidelines, the Procedures and Guidelines must be used to help make decisions in support of the rules.

Procedures and Guidelines

1. General

- **VPMP IT equipment and software** provides eligibility criteria for employees to use mobile phones ordered from the Victoria Police IT Catalogue. As stated in the Policy Rules, employees who are approved to carry a smart phone (e.g. an iPhone) are also required to comply with the procedures outlined below.

- Victoria Police SIM cards must not be used in personally owned devices and personally owned SIM cards must not be used in Victoria Police owned devices.

2. Ordering a new mobile/smart phone

2.1 *Process*

- Mobile/smart phones are to be purchased in accordance with the IT Catalogue through the Victoria Police departmental Telstra Representative.
- Full details on the process for requesting mobile/smart phones and a list of Departmental Telstra Representatives are available on the mobile phone intranet page.
- Work Unit Managers are to approve the request prior to the order being submitted to the Telstra Representative.

2.2 *Funding*

As stated in **VPMP IT equipment and software**, the employee's Work Unit will incur the cost of purchasing a mobile/smart phone as well as extended support and warranty (for example, Apple Care for iPhones). Work units are also responsible for all ongoing operating costs, including data.

3. Use

3.1 *General requirements*

- Victoria Police owned phones:
 - are only to be used for personal activities in accordance with **VPMP Appropriate use of information**
 - should not be connected to non Victoria Police IT equipment unless essential for operational duties.
- Smart phones must only be used in accordance with VPM policy and applicable guidelines including, but not limited to:
 - **VPMG Portable computing devices**
 - **VPM Recording devices**, CCTV and digital asset management
- Devices holding security classified police information must be handled in accordance with **VPMP Information use, handling and storage**.
- Victoria Police information must not be stored or transmitted using Internet based systems or accounts unless specifically authorised by the Information Management Committee.
- Work Unit Managers are to maintain a record of the allocation and use of a handset in the Portable and Attractive Item Register (PAIR).

3.2 Phone security

- Employees are responsible for ensuring that Victoria Police phones are protected from unauthorised access and use at all times.
- Available security functions, such as password/keycode locks, are to be set to automatically activate when the phone is not in use.

3.3 Repairs under warranty and replacement of unserviceable handsets

- Where the device requires repair under warranty, the Work Unit Manager or area Telstra Representative should liaise directly with the device provider, Telstra.
- Although phone handsets are on a three year replacement cycle, replacements should only be obtained if the device is no longer serviceable.
- To replace an unserviceable device, the Work Unit Manager and relevant Victoria Police Telstra Representative need to approve the request.
- Retain the SIM as well as any associated storage media and order a replacement handset using the process detailed available on the mobile phone intranet page.
- All mobile phones must be destroyed in accordance with section 3.4, even if the device is unserviceable.

3.4 Lost or stolen handset

- If a Victoria Police handset is lost or stolen it is to be reported immediately to the Victoria Police IT Helpdesk on 1300 307 082. The helpdesk will organise a remote wipe and deactivation of your handset where possible.
- The loss or theft of the handset is also to be reported to your Supervisor and to the Security Incident Registry, Protective Security in line with **VPMP Protective security incident reporting and management**.
- A new handset must be ordered in line with section 2 of these guidelines.

3.5 Re-allocation or disposal

- Prior to reallocation to another Victoria Police user, the mobile phone handset, SIM card and any other storage media is to be cleansed through a hard delete process. A hard delete provides a more effective data deletion process than the standard user delete processes. Details of where to seek advice on this process is available in G130 Secure mobile phone sanitisation/disposal.
- Mobile/smart phones that have reached the end of their useful life, or cannot be reallocated, must be destroyed in accordance with **VPMP Information review, retention and disposal**.

- The disposal process for mobile/smart phones, SIM cards and other storage media is provided in **G130 Secure mobile phone sanitisation/disposal**.
- Work Unit Managers are to maintain a record of any disposal actions of the handset in the PAIR (Refer to the Workplace Inspection Manual) for Victoria Police Owned devices or Personally Owned Devices where the employee has chosen to use the device for work purposes.

Further Advice and Information

For further advice and assistance regarding these Procedures and Guidelines, contact your local IT Co-ordinator or your supervisor.

Update history

Date of first issue	15/10/13	
Date updated	Summary of change	Force File number
25/03/19	Administrative amendment to change IMSSD to Protective Security.	FF-139207
17/07/24	Administrative amendment as a result of newly published VPM Recording devices, CCTV and digital asset management.	FF-236615