

Victoria Police Manual – Procedures and Guidelines

Portable Computing Devices

Source Policy

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

- VPMP Information access
- VPMP Appropriate use of information

The following references provide additional information or requirements of relevance:

- VPMP Information categorisation collection and recording
- VPMP Information use, handling and storage
- VPMP Information sharing
- 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. Overview

- Portable Computing Devices (PCDs) have the capacity to significantly and positively impact Victoria Police service delivery and working environments. Whilst convenient, their widespread use requires application of appropriate controls to reduce potential risks to Victoria Police information and infrastructure. These risks include, but are not limited to:
 - information stored on PCDs can be easily compromised through the use of malicious software

- the introduction of viruses and other undesirable intrusions to Victoria Police IT infrastructure
 - PCD's portability and small size mean they can be easily misplaced, lost and/or stolen
 - PCD's ability to store huge amounts of information has the potential to expose Victoria Police to grave security risks.
- Victoria Police and all Authorised Users have a duty and responsibility to ensure that Victoria Police information is protected from harm, unauthorised or inappropriate disclosure, while at the same time ensuring that it is available to those who have a legitimate right or need to know.

2. Definitions

- A PCD is any portable device which can store and/or transfer electronic information from one information system resource to another. It includes, but is not limited to:
 - Portable flash memory (referred to as USB keys/sticks, thumb drives, flash cards or memory sticks)
 - External hard drives/storage devices
 - Mobile phones (standard or smart phone)
 - Video or still cameras (equipment mounted, body worn or hand held)
 - Audio recorders
 - Laptops, Tablets or other devices with in-built accessible storage (such as iPod, Personal Digital Assistant)
- In this guideline PCDs do not include the use of equipment as surveillance devices (see **VPMP Investigation support**) or portable recording devices (see **VPM Recording devices, CCTV and digital asset management**) or a standard telephone for voice calls.

3. Information ownership

As stated in **VPMP Appropriate use of information**, any information that is acquired, created, stored or used by individuals in the course of their duties as employees of Victoria Police is owned by the organisation, regardless of whether it is on personally owned equipment or Victoria Police owned equipment.

4. Equipment

4.1 Availability

In accordance with **VPMP Information collection, recording and use**, Victoria Police owned equipment must be used wherever possible.

4.2 *Victoria Police owned PCDs*

- Victoria Police owned PCDs must only be used for personal activities in accordance with **VPMP Appropriate use of information**.
- Victoria Police owned PCDs should not be connected to non Victoria Police networks or IT equipment unless essential for operational duties.
- In accordance with **VPMP Information access**, PCDs that have been connected to a non Victoria Police network or IT equipment should be scanned for viruses prior to the download or access of any information through the Victoria Police network or IT equipment.
- Only approved third party applications/apps may be loaded onto Victoria Police owned PCDs. It is the Authorised User's responsibility to confirm:
 - an application/app is authorised
 - if an exemption to this rule has been approved by the IT Security Advisor for a particular device.
- PCDs must be cleansed of all Victoria Police data or destroyed in accordance with **VPMP Information review, retention and disposal** when:
 - it has reached the end of its useful life
 - prior to being sold or given to a third party.

4.3 *Personally owned equipment*

Victoria Police does not currently have the technological or security capabilities to allow a general "bring your own device" policy.

- Personally owned PCDs that are used to connect to personal or public systems (including home computers or online data storage facilities), regardless of the method of connection, are not to be used to collect, transmit or store Victoria Police information.
- The only exception to the above requirement is:
 - when the device is able to segregate and protect Victoria Police information or used to remotely access the Victoria Police network through approved secure methods (such as Connect.Police tokens or Good for Enterprise), **and**
 - all security and usage requirements for the application/connection are adhered to.
- If an Authorised User chooses to purchase personally owned equipment for operational duties, the equipment should provide the security functions to protect Victoria Police information appropriate to the security classification of the material, such as encryption and password protection or be suitable for the approved secure application/connection tools. See the **Protective Security Portable computing device guide**.

- If an Authorised User chooses to use personally owned equipment for the capture, storage or transmission of Victoria Police information they are to use the device solely for work purposes as:
 - the mixing of personal and official information (such as on a smart phone or tablet) opens the risk of unauthorised access to official information or personal information becoming part of official records. This should be actively avoided unless absolutely necessary.
 - Victoria Police takes no responsibility for the loss or compromise of personal information.
- A personally owned device that has been used to collect or store official information must be cleansed of all data or destroyed in accordance with **VPMP Information review, retention and disposal** when:
 - it has reached the end of its useful life
 - prior to being sold or given to a third party.

4.4 *Lost or stolen devices*

- In the event of a device being lost or stolen, it must be reported immediately to your Supervisor and to the Security Incident Registry, Protective Security in line with **VPMP Protective security incident reporting and management**.
- Any delay in reporting the loss or theft, which results in misuse of the device, may contribute to the Authorised User being held responsible for any costs or damages.

5. Authorised User responsibilities

5.1 *Legislative and mandatory*

Authorised Users have an obligation to use their PCDs in a responsible, informed and safe manner. These responsibilities include compliance with legislative and VPM requirements.

5.2 *General*

- Authorised Users need to be mindful of managing PCDs in a secure manner at all times to protect the information they contain from unauthorised access. Devices should not be left at risk in vehicles or in unsecure locations. Authorised Users may be held liable for any negligence resulting in lost, stolen or damaged units.
- Authorised Users are accountable for their use of PCDs and are responsible for the secure storage, use, transmission, access and disposal of information contained on these devices.
- Information on the device is to be secured by security controls such as encryption and password protection. The security controls are to meet the

minimum requirements for the highest security classification of the information on the device.

- PCDs are to be scanned for detection and removal of malicious software before information is transferred between the device and any Victoria Police networked device.
- Authorised Users are not to use PCDs as formal or informal data backup without approval of the IT Security Advisor.
- Authorised Users are to ensure that all Victoria Police information is deleted from PCDs as soon as the information is transferred to an official system and/or the use of the information on the device is completed.

5.3 *Personally owned equipment*

If an Authorised User does not have access to Victoria Police issued equipment and chooses to use personally owned equipment for any Victoria Police information they are to:

- ensure that their Work Unit Manager has confirmed that Victoria Police issued equipment is not available and has recorded the use of a personal device for work purposes
- acknowledge to the Work Unit Manager, that they understand that the device can not be sold, given or otherwise disposed of until it has been appropriately cleansed of all data and may need to be destroyed, depending on the device (See **VPMG Information and information equipment disposal**)
- ensure the equipment has been setup using all security options available
- ensure that the device is not connected to non Victoria Police networks or IT equipment whilst it contains Victoria Police information unless essential for operational duties
- ensure that Victoria Police information is deleted from the personal device as soon as it has been transferred
- ensure that no unauthorised individual has access to the device while it contains police information
- accept responsibility for any unauthorised access to the Victoria Police information on the device.

6. Work Unit Manager responsibilities

In line with the Workplace Inspection Manual, Work Unit Managers should conduct regular audits to ensure that the PCDs are meeting relevant security requirements and being used appropriately.

Work Unit Managers are to:

- require the use of Victoria Police owned equipment where available
- ensure appropriate allocations of Victoria Police owned PCDs to meet operational requirements are identified and associated budget allocations are requested and justified for their supply and maintenance
- ensure that they purchase only approved devices through approved processes
- conduct a risk assessment prior to approving the use of a personally owned PCD. The risk assessment should:
 - gauge the type of information the device will be storing against the risk of unauthorised access
 - consider appropriate physical and technical security controls, such as password protection, encryption and storage (seeking advice from Protective Security where necessary)
- maintain a record of the devices in use and any disposal actions in the Portable and/or Attractive Item Register (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
- not endorse the use of PCDs as formal or informal data backup practices without the approval of the IT Security Advisor
- ensure, when approving the use of a personally owned device, that Authorised Users confirm they understand that the device can not be sold, given or otherwise disposed of until it has been appropriately cleansed of all data and may need to be destroyed, depending on the device (See **VPMG Information and information equipment disposal**).

Further Advice and Information

For further advice and assistance regarding these Procedures and Guidelines, contact your supervisor or Protective Security.

Update history

Date of first issue	15/10/13	
Date updated	Summary of change	Force File number
25/03/19	Administrative amendment to reflect name change from 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