

Chief Commissioner's Instruction

The following instruction is issued pursuant to the powers of the Chief Commissioner under section 60, Victoria Police Act 2013. This Chief Commissioner's Instruction was originally published on the Victoria Police intranet on 23 October 2017 and is effective from that date. It remains in effect until it is formally cancelled or incorporated into the Victoria Police Manual.

CCI 10/17 Mobile device deployment

Context

The mobile device and IRIS suite of applications have been developed by the BlueConnect project team in order to change the way members access information. The IRIS application will provide members in the field with direct access to existing Victoria Police information sources on a mobile device, with a user friendly interface.

Mobile devices will be deployed in stages to specific work units across the organisation.

These instructions support that deployment by providing guidelines to users and work unit managers.

Contents

Context.....	1
Contents	1
Scope and application	1
References.....	1
Definitions.....	2
Responsibilities and procedures.....	2
Allocation	2
User responsibilities.....	2
Work unit manager responsibilities	4
Loss, theft or damage.....	5
Information Security	5
Functionality	6
Further advice and information.....	6

Scope and application

This CCI applies to users and work unit managers involved in mobile device deployment.

References

This CCI is supported by and should be read in conjunction with the following:

- VPMP Information access
- VPM Information categorisation, collection and recording
- VPMP Managing equipment
- VPMP Information use, handling and storage
- VPMP Appropriate use of information
- VPMP Information management and information security

Definitions

The following definitions apply to this CCI:

- **Mobile device** –an Apple iPhone, iPad Mini or similar mobile device authorised for use during the deployment.
- **User** – an authorised police member who is gazetted to or holding a position at a work unit or location involved in the deployment.
- **Work unit manager** – an employee who is responsible for the station, unit or workplace involved in the deployment.

Also refer to the general [VPM Dictionary](#) for definitions and acronyms.

Responsibilities and procedures

Allocation

1. Mobile devices are:
 - deployed to various work units, as determined by BlueConnect
 - allocated to users who hold a position at a work unit involved in the deployment
 - on personal issue to the user unless re-allocated or removed. Refer to paragraph 12 in relation to re-allocation procedures
 - able to be taken home and utilised for reasonable personal use (RPU)
 - to be physically secured and cared for by the user, whether on or off duty.

User responsibilities

Use

2. The table below outlines the circumstances when the mobile device may be used.

Situational awareness	Users must: • maintain awareness of persons, vehicles and objects around them while using their mobile device • not use their mobile device if an operational situation is unknown or uncontrolled.
All use	Users are subject to VPMP Professional and ethical standards at any time their mobile device is used, whether on or off duty or whether the use is work related or personal.
On duty use	Users: • must use their mobile device in accordance with VPMP Information management and information security • must ensure that their mobile device is available and carried during operational shifts for use in the execution of official police duties • Should not use their mobile device: - as a replacement for radio communications, but may be used for direct communication between operational areas where radio communications are impractical or not appropriate

	- while driving a motor vehicle.
Off duty use	Users are: • not on stand-by or expected to perform duties or respond when they are off-duty • not obliged or expected to: - check or respond to work related emails or text messages - make or receive work related telephone calls - use any work related application outside rostered work time • encouraged to turn off their mobile device or use other functions to avoid the interruption of their personal time. Options include: - turning the device ringer level to silent - using 'out of office' functions on email applications (if applicable).
Reasonable personal use	On duty: • personal use should be short and discrete, without interfering with duties. Off duty: • reasonable use of the telephone, messaging and internet functions (dependent upon device type) as defined in VPMG managing equipment • consistent with the principles of VPMG Use of email, VPMG Use of internet and VPMG Social media and online engagement
Unreasonable personal use	• International calls and iMessage are not enabled on the mobile device • iOS Personal Hotspot feature, otherwise referred to as 'tethering' must not be activated on the device.

Procedures

- Users must ensure that their mobile device:
 - remains in their control or is reasonably secured, at all times
 - is sufficiently charged
 - is updated with the most recent software and security updates
 - is available for use during each rostered shift.
- The mobile device should not be:
 - left unattended in private vehicles
 - left within sight in an unattended police vehicle
 - left in areas within police premises which are accessible by the general public (e.g. reception areas, interview rooms or other common areas)
 - given to another person, including other Victoria Police employees.
- If the user wishes to leave their mobile device in the work place rather than take it with them off-duty, the user should:
 - store the device in their correspondence locker (or similar area), or
 - consult with the work unit manager to arrange alternative local storage of the device.

Accessories

6. The following accessories are supplied with the mobile device:
 - a SIM card
 - protective case, including screen protector
 - charging cable and set of headphones (if applicable).
7. Unless directed by the IT Helpdesk, users are not to:
 - remove the device from the protective case
 - remove the SIM card
 - use unauthorised accessories.
8. Users may:
 - order replacement or additional consumables as per the instructions on the BlueConnect Mobile Technology intranet page.

Work unit manager responsibilities

9. Mobile devices will be managed by Motorola Solutions.
10. Work unit managers are not expected to maintain a database or register of devices on issue to their workplace.
11. The work unit manager is to:
 - distribute the mobile devices to users within their work unit
 - Regularly check the physical state of the device and its accessories to ensure they are all fit state for use
 - Regularly check the work unit device management reports, as per the instructions on the BlueConnect Mobile Technology intranet page, in order to review the following:
 - device allocation to position number
 - IRIS application utilisation
 - IRIS application log in history.
12. If a user:
 - is on extended leave or seconded (more than 3 months)
 - permanently leaves a work unit involved in the deployment and there is another user replacing themthe work unit manager is to oversight the:
 - collection of the mobile device from the user
 - removal or backing up of all law enforcement data from the device to ensure that no evidentiary material is lost in the re-allocation process
 - re-distribution of the device to the new user coming into the position
 - new user to contact the IT Helpdesk (1300 307 082), who will assist with the re-allocation of the device.
13. If there is no user to fill a position, the work unit manager should store the device locally, pending re-allocation.

Loss, theft or damage

14. Security and retention of the mobile device is never to take priority over safety. Due to the nature of operational duties, it is understood that incidental damage to the device may occur. If so, the following applies:

Loss/Theft	The user must: • take all reasonable steps to locate their mobile device • as soon as possible, notify: - the Victoria Police IT Helpdesk who will manage: ▪ locking the device ▪ tracking the device to identify its location, so it may be recovered by the user (if applicable) ▪ remote wipe of the device, if it is unable to be located (if applicable) ▪ allocation of a replacement device - their direct supervisor - the work unit manager who is responsible for the device - the Security Incident Registry by submission of a T200 SIR Incident Report. The work unit manager must: • ensure that the user contacts the IT Helpdesk immediately • monitor the submission of the appropriate reports.
Damage	The user must: • as soon as possible: - notify the Victoria Police IT Helpdesk of the damage - manage the return and allocation of a replacement mobile device by completing all instructions from the Helpdesk. • before the end of the rostered shift (or if damage occurs while off duty, by the end of the next rostered shift) prepare a report for the work unit manager detailing the circumstances of the damage. Work unit manager must: • monitor users in their work unit for excessive loss or damage.

Information Security

15. As per the Information Management and Security VPMs, users must adhere to the following principles when accessing Law Enforcement Data:
- only access and use Victoria Police information held electronically and/or in hard copy, where they have a demonstrable, legitimate business need which is directly related to the performance of their current duties with Victoria Police
 - users must not let private interests interfere with their responsibilities as authorised users of Victoria Police information and information systems
 - users are responsible for the security of Victoria Police information that they access or hold. They must treat any information captured, copied, deleted, added, used or disposed of sensitively and professionally with regard to individuals' right to privacy and any security classification requirements.

Functionality

16. Photographs and videos taken on the mobile device while on-duty:
 - remain Victoria Police official information
 - must be:
 - managed with in accordance with **VPM Information categorisation, collection and recording**
 - removed from the device at the first opportunity and stored on an appropriate Victoria Police Network server, portable computing device or hard media
 - permanently deleted from the device by the user, once uploaded and/or backed up.
17. Personal photographs and video should be removed from the device routinely to ensure that data is not lost in the event of a remote data wipe. Victoria Police takes no responsibility for the loss of personal data stored on the mobile device.
18. In order to perform an update, the user:
 - will be prompted by a notification on the device when an update is available or required
 - should refer to the BlueConnect Mobile Technology intranet page for instructions on how to complete an update.
19. Updates should be conducted while on duty, at the start, or prior to the conclusion of a rostered shift. Whilst downloading and installing an update, the mobile device may not be available for operational duties.
20. The following is applicable to the mobile device:
 - the standard Apple App Store will be disabled.
 - applications will be available for download through the dedicated Victoria Police App Store
 - the phone number will be blocked for outgoing voice calls
 - voice mail and global roaming will not be enabled on the device.
21. If a user can establish a genuine business need for either voicemail or global roaming to be enabled, a report outlining that need should be submitted to work unit manager for endorsement. Refer to the BlueConnect Mobile Technology intranet page for the application process.

Further advice and information

For further advice and assistance with this instruction, refer to the BlueConnet Mobile Technology intranet page.