IN THE MATTER OF THE ROYAL COMMISSION INTO FAMILY VIOLENCE

ATTACHMENT WS AH-3 TO JOINT STATEMENT OF ASSISTANT COMMISSIONER WENDY MAREE STEENDAM AND SENIOR SERGEANT AILSA CAROLINE HOWARD

Date of document: 3 August 2015
Filed on behalf of: the Applicant
Prepared by:
Victorian Government Solicitor's Office
Level 33
80 Collins Street
Melbourne VIC 3000

[redacted]

This is the attachment marked **'WS AH-3'** produced and shown to **WENDY MAREE STEENDAM** and **AILSA CAROLINE HOWARD** at the time of signing their Joint Statement on 3 August 2015.

Before me: [redacted]

[redacted]
An Australian legal practitioner
within the meaning of the
Legal Profession Uniform Law (Victoria)

Attachment WS AH-3

Victoria Police Manual – Policy Rules

Appropriate use of information

Context

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. This information must at all times be used appropriately and kept secure from unauthorised access. This security and appropriate use of information is essential to the organisation's credibility and its ability to provide an effective and professional law enforcement service to the Community.

All individuals who are authorised to access Victoria Police information, play an important role in maintaining the security of Victoria Police information and information systems and, as such, must familiarise themselves with their responsibilities in keeping police information secure and protected at all times from unauthorised access.

Victoria Police regards breaches or violations of this policy and/or the misuse of its information resources and privileges as particularly serious and may lead to disciplinary consequences including termination of appointment.

The *Victoria Police Act 2013* prohibits current and former police employees, as well as contractors and service providers, from accessing, using or disclosing police information if it is their duty not to access, make use of, or disclose the information. Breaches or violations of this policy and/or the misuse of information resources and privileges are particularly serious and may lead to management or disciplinary action, or charges under sections 227 and 228 of the *Victoria Police Act 2013.*

Application

Policy rules are mandatory and provide the minimum standards that employees must apply. Non-compliance with or a departure from a policy rule may be subject to management or disciplinary action. Employees must use the **Professional and Ethical Standards** to inform the decisions they make to support compliance with policy rules.

These policy rules apply to all Authorised Users granted access police information.

Rules and Responsibilities

1. Appropriate access / use of information

- Employees and other Authorised Users must 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.

- Authorised Users must not let private interests interfere with their responsibilities as Authorised Users of Victoria Police information and information systems.

- Authorised Users are responsible for the security of Victoria Police information that they access or hold. They must treat any information copied, deleted, added, used or disposed of sensitively and professionally with regard to individuals' right to privacy and any security classification requirements.

2. Personal use of resources

- Authorised Users must not use Victoria Police information systems to access or use law enforcement data or other official information, directly or indirectly, for unofficial reasons or personal interest.

- Authorised Users may use Victoria Police information systems to create, transmit or access public domain information for personal reasons, provided that the use:
  - is incidental, occasional and does not interfere with work responsibilities
  - constitutes a minor use of Victoria Police system resources
  - is consistent with the principles of these Policy Rules, **VPMG Use of email, VPMG Use of internet** and **VPMG Social media and online engagement**
  - is consistent with any conditions of use imposed by the local Work Unit Manager.

- Any personal information created, stored and/or transmitted on Victoria Police information systems is treated as Victoria Police information, and as such Victoria Police reserves the right to:
  - access, copy, and/or delete all such information for any purpose
  - disclose that information to any party deemed appropriate by the System or Information Owner.

3. Authorised User responsibilities

To ensure the confidentiality, integrity and availability of Victoria Police information and information systems Authorised Users:

- must only access and use Victoria Police information and information systems in accordance with **VPMP Information access** and this policy

- must not take unacceptable risks in the transfer and storage of information, see **VPMP Information use, handling and storage**

- are responsible for the information they create and store:
  - in computer datasets on a mini-, mid-range, mainframe or personal computers
  - in network folders/directories (for example G: H: and P: drives)
  - on storage media of any portable computing device or peripheral device
  - on any other removable storage medium
  - in hardcopy documents and files
- must only permit Victoria Police information to be viewed by personnel who have been authorised to access that information
- are accountable for any activity performed using their passwords or access privileges. Therefore, they must ensure that:
  - they do not leave their computer unattended without logging-off or using password protection
  - their passwords are created and managed to prevent disclosure to other persons; see **VPMG Password management.**
- must not access, create, copy, forward or store information that contains inappropriate or offensive material, or links to such material or websites on Victoria Police information systems, except where there is a legitimate business purpose endorsed by the Work Unit Manager. Inappropriate or offensive material includes but is not limited to:
  - material containing any discrimination or vilifying language, images or sounds relating to an individual's or group's personal characteristics, whether actual or presumed, including race, disability, physical features, sexual orientation, gender identity, religious or political beliefs, national origin, marital or parental status, pregnancy or breastfeeding or age
  - any material the circulation of which would constitute a breach of the *Equal Opportunity Act 2010 (Vic)* and/or the *Racial and Religious Tolerance Act 2001 (Vic)*
  - any material the circulation or disclosure of which would be incompatible with a person's human rights under the *Charter of Human Rights and Responsibilities 2006 (Vic)*
  - obscene, pornographic, erotic, sexually explicit, violent, defamatory, offensive, insulting, threatening or harassing language, images or sounds
  - any other material which a reasonable person would find offensive; see **VPMP Bullying, discrimination and harassment.**
- must not introduce information that contains inappropriate or offensive material, or links to such material or websites to Victoria Police information systems, except where there is a legitimate business purpose endorsed by the Work Unit Manager

- must not subscribe to, or participate in, social networking or create accounts with or access web-based email services (such as hotmail) using Victoria Police resources, except where there is a legitimate business purpose endorsed by the Work Unit Manager

- must have regard to any policies, standards, procedures, guidelines and/or security controls to specific information systems that they have access to, including:
  - **VPMG Information use, handling and storage**
  - **VPMG Use of email**
  - **VPMG Use of internet**
  - **VPMG Social media and online engagement**
  - any instructions issued by the relevant System or Information Owner.

4. Work Unit Managers' responsibilities

Work Unit Managers are responsible for:

- engendering and promoting a workplace culture, environment and work practices that value and enhance the security, privacy, confidentiality, integrity and availability of the information under their management

- ensuring that personnel in their work unit are aware of, and comply with, the Victoria Police Information Management and Information Security Policies

- ensuring new personnel under their management are given adequate training in information management and information security and their responsibilities under the VPM

- ensuring departing personnel are aware on their ongoing obligation not to disclose police information under the *Victoria Police Act 2013*

- ensuring that information and information system components located in their work units are kept secure from theft, damage, loss and unauthorised access

- ensuring that workplace inspections include adequate monitoring to identify potential instances where policy rules are not being followed

- ensuring they (or their nominated delegate) only authorise access or variations to access to the information created, used and stored in the work unit or in the network folders/directories under their responsibility, as required **VPMP Information access**

- conducting audits of access to their physical location and network folders/directories they are responsible for, to ensure only those

authorised users with a current business need have access to information stored there

- ensuring that the controls used to maintain the security of information is commensurate with the sensitivity and any official information that requires a higher degree of security and an increased level of protection is security classified.

5. Misuse of information or information systems

- All Authorised Users must report misuse of Victoria Police information or information systems to the appropriate Work Unit Manager and/or as a security incident.

- The misuse of Victoria Police information and information systems includes, but is not restricted to, the following:
  - accessing any Victoria Police information (or information accessible to them as a representative of Victoria Police) for which they do not have an authorised Victoria Police business need requiring that specific access
  - attempting to use previously authorised access privileges following termination of employment or contract with Victoria Police, irrespective of whether or not those access privileges have been revoked and/or removed
  - attempting to modify or remove information or information system resources without proper authorisation
  - attempting to use, or using, any other person's UserID
  - accessing information or information systems without proper authorisation
  - attempting to test, bypass or defeat any security safeguards established to protect Victoria Police information or information systems, except as authorised as part of security control assessment
  - circumventing or attempting to circumvent assigned resource limits, logon procedures or assigned privileges
  - using information systems for purposes other than those for which they were intended or authorised
  - sending fraudulent computer mail, breaking into another user's mailbox or reading their mail without permission
  - sending any fraudulent electronic transmissions
  - violating any software licence agreement or copyright
  - harassing or threatening other users or interfering with their access to Victoria Police information systems
  - taking advantage of another user's naivety or negligence to gain access to information systems for which they have not been authorised

- encroaching on others' use of information systems through such activities as sending excessive or frivolous messages or printing excessive copies
- disclosing or removing third-party proprietary information.

Quick Links

- VPMP Information access
- VPMG Information system access
- VPMG Password management
- VPMG System access for specific groups
- VPMG Use of email and internet
- VPMG Clear desk principles
- VPMG Portable computing devices

Further Advice and Information

For further advice and assistance regarding these Policy Rules, contact Information Management, Standards and Security Division.

Update history

Date of first issue	03/12/2012	
Date updated	**Summary of change**	**Force File number**
	This is a new instruction arising from a comprehensive review by IMSSD of the entire *IT, Information Management and Security* section of the VPM	069562/11
18/11/13	References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	069562/11
28/02/14	References to redundant instruments following IMSSD review have been updated with corresponding new instruments.	069562/11
01/07/14	Legislative reference updates due to the commencement of the *Victoria Police Act 2013*.	069562/11
22/12/14	VPM reference updates due to implementation of VPMP Bullying, discrimination and harassment.	068126/11