Information privacy

Source Policy

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

- VPMP Information sharing
- VPMP Appropriate use of information

The following references provide additional information or requirements of relevance:

- *Privacy and Data Protection Act 2014*
- *Health Records Act 2001*
- VPMP Information access
- VPMP Information categorisation, collection and recording
- 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. Overview

- The *Privacy and Data Protection Act 2014* (PDPA) and the *Health Records Act 2001* (HRA) deal with the handling and management of personal and health information in Victoria, including by Victoria Police employees.

- Victoria Police must comply with these Acts, however at times employees may be exempt because:
  - under s.15, PDPA (refer section 4 below), there is a law enforcement exemption provision that applies in certain circumstances
  - in some cases there may be a specific provision in another Act that applies to the handling of information. If this occurs the specific provision takes precedence over these Acts.
- All Victoria Police employees should understand the basic elements of these Acts to facilitate compliance and to minimise breaches or complaints.

2. Privacy and Data Protection Act

2.1 Personal information

- Personal information is:
  - information or opinion (including that forming part of a database) that is recorded in any form whether true or not, about an individual whose identity is apparent, or can be reasonably ascertained from the information or opinion, but does not include health information
  - information only applicable to a natural person. It does not relate to deceased persons.

2.2 Information Privacy Principles

The Information Privacy Principles (IPPs) are contained in Schedule 1 of the PDPA. These principles provide practical guidance on how to comply with the PDPA. Information regarding the IPPs is outlined below.

2.3 Collection of information (IPP 1)

- Employees must only collect personal information if the information is necessary for one or more of Victoria Police's functions or activities (IPP 1.1). The collection must only be by lawful and fair means and not in an unreasonably intrusive way (IPP 1.2).
- Where personal information is collected for reasons other than law enforcement or community policing functions, the subject should be provided with collection information as outlined in IPP 1.3.
- Where the law enforcement exemption provision applies, there is no requirement to inform an individual that collection has taken place, or of the source, purpose or reason for the collection of information.

2.4 Use and disclosure of information (IPP 2)

- The PDPA permits organisations to use and disclose personal information for the primary purpose for which the information was collected.

- IPP 2.1 specifies circumstances where personal information may be used or disclosed for a secondary purpose.

- Victoria Police is exempt from this if the law enforcement exemption provision applies (s.15 PDPA). Details regarding the law enforcement exemption provision are provided in section 4 below.

- All Victoria Police employees must also comply with Victoria Police policies on release of information, refer **VPMP Information sharing**.

- The **Privacy Information Sharing Guide** assists Victoria Police staff in making a decision when receiving a request for information from an external agency.

2.5 Data quality (IPP 3)

Victoria Police must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date. In line with **VPMP Information categorisation, collection and recording**, employees must ensure the data quality of all information.

2.6 Data security (IPP 4)

- Victoria Police must take reasonable steps to:
  - protect the personal information it holds from misuse, loss and unauthorised access, modification or disclosure
  - destroy or permanently de-identify personal information if it is no longer required for any purpose.

- In accordance with **VPMP Information access** and **VPMP Appropriate use of information**, employees are to ensure that computer screens and other data sources containing personal information are not viewable to the public in Watch-houses, police station receptions or any other Victoria Police site where members of the public may be allowed. Data sources may include Attendance Register, printer output trays, photograph boards, notice boards and whiteboards.

2.7 Openness (IPP 5)

Victoria Police must set out in a document clearly expressing policies on its management of personal and/or health information and must make it available to anyone who requests it. The document (Information Privacy Statement & Health Records Statement) may be provided to any person, including members of the public on request. It is available from the Privacy Unit or on the Victoria Police website.

2.8 Access to and correction of information (IPP 6)

- Where Victoria Police holds personal information about an individual, the individual can seek access to and correct the information through the Freedom of Information Office. This is regulated by the *Freedom of Information Act 1982* and not IPP 6.

- 'Access' to information under the PDPA refers to access by a person to his or her own information. The 'disclosure' of information under the PDPA refers to the giving of an individual's personal information to another person (i.e. a third party).

2.9 Unique Identifiers (IPP 7)

A unique identifier is a number or code that identifies people across public sector organisations (such as JAID/MNI number). This IPP prohibits the use of unique identifiers between organisations, except in specific circumstances. Victoria Police utilises unique identifiers so that it can carry out its functions efficiently.

2.10 Anonymity (IPP 8)

- If it is lawful and practicable, a person must have the option of not identifying themselves when entering transactions with Victoria Police. However, specific statutory provisions such as s.456AA, *Crimes Act 1958* (requirement to provide name and address) and s.59, *Road Safety Act 1986* (requirement to produce drivers' licence) take precedence over the PDPA.

- Activities that involve community engagement in policing initiatives may also fall within the scope of community policing functions. Guidance regarding community policing functions may be obtained in section 4.1 or from the Privacy Unit.

2.11 Transborder data flows (IPP 9)

- Where Victoria Police is transferring personal information to another organisation outside of Victoria, it must ensure that the receiving organisation has equivalent privacy protection, and that the information transferred will be protected.

- Where it is reasonably believed necessary, Victoria Police is exempt under s. 15 PDPA from its obligation in respect of its law enforcement functions and activities.

- However, precautions related to the security of personal information are to be undertaken in all transborder data exchanges by Victoria Police.

2.12 Sensitive information (IPP 10)

- Sensitive information (defined in schedule 1 PDPA) is information or opinion about an individual's:
  - racial or ethnic origin
  - political opinions/membership of a political association
  - religious beliefs or affiliations
  - philosophical beliefs
  - membership of a professional or trade association
  - membership of a trade union
  - sexual preferences or practices
  - criminal record.
- An organisation may only collect sensitive information in restricted circumstances. There are special restrictions on the collection of this information.
- Where it is believed reasonably necessary, Victoria Police is exempt under s. 15 PDPA from those restrictions where sensitive information is collected for a law enforcement or community policing function or activity.

3. Health Records Act

3.1 Health information

- Health information (defined in s. 3 HRA), in summary, is information or opinion about an individual's:
  - physical health
  - mental health
  - psychological health
  - disability
  - personal information collected to provide a health service.
- Health information is more strictly regulated than other personal and sensitive information. Unlike the provisions set out in s.15 PDPA, Victoria Police does not have a general exemption to collect, use or disclose health information.
- The HRA applies to natural persons as well as an individual who has been dead for 30 years or less, so far as reasonably capable of doing so, in the same way as it applies to an individual who is not deceased.

3.2 Health Privacy Principles

- The HRA is based on eleven health privacy principles (HPPs). The HPPs are in Schedule 1 of the HRA. The most relevant HPPs to Victoria Police relate to collection, disclosure, access and security. Specifically, Victoria Police:

- may only collect information in accordance with HPP 1. The subject must be provided with collection information as outlined in HPP 1.4
- may use and disclose health information about an individual for the primary purpose for which the information was collected in accordance with HPP 1.1
- may only disclose information in accordance with HPP 2
- must take reasonable steps to protect the health information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4. Law Enforcement Exemption Provision

4.1 PDPA

- Section 15 of the PDPA exempts Victoria Police employees from complying with IPP 1.3 to 1.5, 2.1, 6.1 to 6.8, 7.1 to 7.4, 9.1 or 10.1 if they believe on reasonable grounds that the non-compliance is necessary for the purpose (amongst other purposes):
  - of its, or any other law enforcement agency's, law enforcement functions or activities
  - of its community policing functions.
- Where possible, Victoria Police should attempt to comply with the IPPs, before relying on s. 15 PDPA.
- The phrase 'community policing functions' is not defined in the PDPA, however the following can be used as examples of community policing functions:
  - licensing investigations
  - location of missing persons
  - providing necessary responses in public emergency and disaster situations
  - locating next of kin if required.
- Guidance regarding what constitutes community policing functions can be found in the *Privacy and Data Protection Bill 2014 Explanatory Memorandum*.

4.2 Precedence of other legislation

- Where there is any inconsistency between the privacy legislation and a specific privacy provision in another Act, the specific provision takes precedence (s.6, PDPA and s.7, HRA).

4.3 Consent

- If a person consents to any action or process, the privacy restrictions do not generally apply. Consent may be express or implied.

5. Flexibility Mechanisms

The PDPA contains three new methods to obtain temporary authorisations for acts or practices that would otherwise breach privacy requirements. The new instruments are:

- **Public Interest Determination** (PID) & Temporary Public Interest Determination (TPID) – these are determinations that the public interest of engaging in an act or practice that may contravene a specified Information Privacy Principle (IPP) (other than IPP 4 or 6) substantially outweighs the public interest in complying with that IPP. Engaging in an act or practice that is permitted by a public interest determination will not be an interference with privacy

- **Information Usage Agreement** (IUA) – IUAs can either:
  - modify the application of specified IPPs (other than IPP 4 (security) or IPP 6 (access and correction)) to, or exempt from the application of such IPPs, specified acts or practices involving the handling of personal information, or
  - provide that an act or practice that is covered by the arrangement is required or authorised for the purposes of an information handling provision in another Act.

- **Certification:**
  - provides the ability to have the CPDP formally certify that specified acts or practices (e.g. a process or information exchange) are compliant with the IPPs
  - the effect of certification is that a person who engages in the act or practice in good faith does not contravene the specified requirement(s). This may be able to assist in reassuring other agencies that are reluctant to provide data exchanges with Victoria Police that the information sharing is not in contravention to the IPPs.

These exemption options are in addition to the Law Enforcement exemption provision contained within the PDPA. Based on this, the application by Victoria Police for a PID, TPID, IUA or Certification is expected to be infrequent.

Should any area believe that they have a requirement to apply for a PID, TPID, IUA or a certification under the PDPA, they must engage with the Privacy Unit, Protective Security to develop an application and for submission to the CPDP via the Chief Information Officer. Work Units are not to contact the CPDP directly.

6. Complaints

6.1 Avenues for complaints

- If an individual believes that Victoria Police has not handled their personal and/or health information in accordance with an IPP or HPP, they may make a complaint. Complaints can be made to:
  - Victoria Police
  - the Independent Broad-based Anti-corruption Commission (IBAC)
  - the Commissioner for Privacy and Data Protection or Health Services Commissioner.
- For advice on information privacy complaints or investigations, contact the Privacy Unit.

6.2 Informal complaints

- Simple matters that may result from a misunderstanding about police procedure or poor communication can be addressed quickly without substantial investigation.
- Employees who receive such complaints should:
  - attempt to resolve the matter informally with the complainant
  - notify the Privacy Unit of the nature and outcome of the complaint.

6.3 Formal complaints

- Matters that are more complex or serious may require a proper investigation.
- Employees should take these complaints in writing and refer them to the Privacy Unit. The investigation will be:
  - coordinated by the Privacy Unit
  - conducted by either the Privacy Unit or the area where the complaint arose
  - conducted in accordance with the Victoria Police Privacy Complaints Policy.

7. Memorandum of Understanding

- The use of a Memorandum of Understanding (MOU), when information sharing, is not mandatory. However, to clarify specific processes and ensure the organisations agree to comply with applicable CLEDS Standards with regards to security law enforcement data, Victoria Police may enter into an MOU with organisations to aid their investigations and functions.
- With or without an MOU, **VPMP Information sharing** documents the essential requirements.

- All MOUs must be developed in accordance with **VPMP Formal arrangements with external organisations**.
- Information on how to obtain a current list of MOUs can be found on the VPM intranet site.

Further Advice and Information

For further advice and assistance regarding these Procedures and Guidelines, contact your Work Unit Manager or the Privacy Unit, Protective Security.

Update history

Date of first issue	15/10/13	
Date updated	**Summary of change**	**Force File number**
28/09/15	Incorporation of CCI 11/14 Privacy and Data Protection Act 2014	FF-097617
25/03/19	Administrative amendments to reflect name change from IMSSD to Protective Security.	FF-139207