

Victoria Police Manual

The Victoria Police Manual is issued under the authority of the Chief Commissioner of Police in s.60, Victoria Police Act 2013. Non-compliance with or a departure from the Victoria Police Manual may be subject to management or disciplinary action. Employees must use VPM Professional and ethical standards to inform the decisions they make to support compliance.

Information privacy

Context

The purpose of this policy is to provide guidance to employees regarding the importance of information privacy, including police information and health information. This includes instructions supporting compliance with the *Privacy and Data Protection Act 2014* and *Health Records Act 2001*, which govern the handling and management of personal and health information in Victoria.

This policy includes:

- the legislative framework for the collection, use and disclosure of personal information
- an explanation of the information privacy principles that must be considered by Victoria Police when handling personal information
- the legislative framework for the collection, use and disclosure of health information
- exemptions from the information privacy principles
- guidance for managing information privacy complaints
- an overview of formal information sharing arrangements between agencies.

Contents

Context	1
Contents	1
Definitions	1
Scope and application	2
Responsibilities and procedures	2
1. <i>Privacy and Data Protection Act 2014</i>	2
2. <i>Health Records Act 2001</i>	5
3. <i>Law Enforcement Exemption Provision</i>	5
4. <i>Temporary authorisations</i>	6
5. <i>Complaints</i>	7
6. <i>Memorandum of Understanding</i>	7
Related documents	8
Further advice and information	8
Update history	8

Definitions

Access – Under the *Privacy and Data Protection Act 2014* (PDPA), refers to access by a person to their own information.

Disclosure – Under the PDPA and in the context of this policy, refers to the giving of an individual's personal information to another person (i.e. a third party). This differs from disclosure in criminal and civil proceedings.

Health information – defined in s.3, *Health Records Act 2001* (HRA), is information or opinion about a person's physical health, mental health, psychological health, disability or personal information

collected to provide a health service.

Information privacy principles (IPPs) - 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 at section 1 of this policy.

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

Sensitive information - defined in schedule 1 PDPA as personal information about a person'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.

Scope and application

This policy applies to all Victoria Police employees.

Responsibilities and procedures

1. *Privacy and Data Protection Act 2014*

The PDPA provides for the responsible collection and handling of personal information in the Victorian public sector, including Victoria Police. As a law enforcement agency, Victoria Police has specific obligations relating to law enforcement data and has some exemptions from compliance with certain IPPs for law enforcement purposes (refer to section 3.1 of this policy). This policy instructs employees regarding IPPs relevant to Victoria Police; employees should refer to the Privacy intranet site for further information on the IPPs more broadly.

1.1 *Collection of information (Information Privacy Principle 1)*

- IPP 1.1 - Employees must only collect personal information if the information is necessary for one or more of Victoria Police's functions or activities.
- IPP 1.2 - The collection must only be by lawful and fair means and not in an unreasonably intrusive way (IPP 1.2).
- IPP 1.3 - Where personal information is collected for reasons other than law enforcement or community policing functions, the person should be provided with collection information as outlined in this IPP. IPP 1.4 – 1.5 - Where the law enforcement exemption provision applies, there is no requirement to inform the person that collection has taken place, or of the source, purpose or reason for the collection of information if this has not been obtained from the person directly.

1.2 *Use and disclosure of information (Information Privacy Principle 2)*

- The PDPA permits organisations to use and disclose personal information for the primary purpose for which the information was collected.
- IPP 2.1 - Permits information to be used or disclosed for a secondary purpose in certain circumstances including:
 - where the secondary purpose is related to the primary purpose for collection and the person whose information was collected would reasonably expect the use or disclosure (IPP 2.1(a))

- where the individual to whom the information relates consents to the use or disclosure (IPP 2.1(b))
- where the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare or a serious threat to public health, public safety or public welfare (IPP 2.1(d))
- where there is reason to suspect that unlawful activity has been, is being or may be engaged in and the use or disclosure of the information is a necessary part of investigating the matter or reporting it to relevant persons or authorities (IPP 2.1(e))
- where the use or disclosure is required or authorised by or under law (IPP 2.1(f))
- where the use or disclosure is reasonably necessary by or on behalf of a law enforcement agency for:
 - the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing a penalty or sanctions or
 - for the enforcement of laws relating to the confiscation of the proceeds of crime or
 - for the protection of the public revenue or
 - for the prevention, detection, investigation or remedying of seriously improper conduct or
 - for the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal (IPP 2.1(g)).
- Victoria Police is exempt from information privacy principle 2 if the law enforcement exemption provision applies (s.15, PDPA). Details regarding the law enforcement exemption provision are provided in section 3 of this policy.
- All employees must comply with **VPM Information security** regarding release of information.
- Employees should refer to the Privacy Information Sharing Guides available on the Digital Services and Security Department (DSSD) intranet page for guidance in making a decision when receiving a request for information from specific external agencies.

1.3 *Data quality (Information Privacy Principle 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.

1.4 *Data security (Information Privacy Principle 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 **VPM Information security**, employees must ensure that computer screens and other data sources containing personal information are not viewable to the public, including in public places, 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.

1.5 ***Openness (Information Privacy Principle 5)***

Victoria Police documents its management of personal and/or health information in the Information Privacy Statement and Health Records Statement. The Statement must be made available to anyone who requests it, including members of the public. The Statement is available on the Victoria Police website.

1.6 ***Access to and correction of information (Information Privacy Principle 6)***

Where Victoria Police holds personal information about an individual, they can seek access to and correct the information through the Freedom of Information Office. This is regulated by the *Freedom of Information Act 1982* (FOI Act) for Victoria Police and not IPP 6, which governs organisations not covered by the FOI Act.

If a person wants to access or correct information, employees should refer them to the Victoria Police website which details processes for members of the public to submit a request via the Victorian Government online portal or emailing foi@police.vic.gov.au.

1.7 ***Unique Identifiers (Information Privacy Principle 7)***

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

1.8 ***Anonymity (Information Privacy Principle 8)***

- If it is lawful and practicable, a person must have the option of not identifying themselves when entering transactions with Victoria Police unless specific powers to require this apply. For example, 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. Refer to section 3.1 of this policy for guidance regarding information related to community policing functions or the Privacy Unit, DSSD.

1.9 ***Transborder data flows (Information Privacy Principle 9)***

- The purpose of IPP 9 is to ensure that when personal information travels outside Victoria it remains subject to privacy protections.
- Where Victoria Police transfers 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 (IPP 9.1(a)).
- 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 must be undertaken in all transborder data exchanges by Victoria Police.

1.10 ***Sensitive information (Information Privacy Principle 10)***

- Victoria Police may only collect sensitive information where:

- the individual gives consent (IPP 10.1(a))
- the information is required or authorised under law (IPP 10.1(b))
- the information is necessary to lessen or prevent a serious threat to the life or health of an individual (IPP 10.1(c)) or
- the information is necessary for legal or equitable claims (IPP 10.1(d)).
- 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. Refer to the DSSD intranet Privacy page for further information.

2. Health Records Act 2001

The Health Records Act promotes fair and responsible handling of health information in Victoria by governing privacy protections, providing people with a right of access and establishing a framework for the resolution of health information handling complaints. This policy instructs employees regarding Health Privacy Principles (HPPs) relevant to Victoria Police; employees should refer to the Privacy intranet site for further information on the HPPs more broadly.

2.1 Health information

- 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 in the same way to natural persons as well as a person who has been dead for 30 years or less.vg

2.2 Health Privacy Principles

- The HRA is based on eleven HPPs. The HPPs are in Schedule 1 of the HRA and can be found on the DSSD intranet Privacy page. 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 person must be provided with collection information as outlined in HPP 1.4
 - may use and disclose health information about a person 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.

3. Law Enforcement Exemption Provision

3.1 Privacy and Data Protection Act 2014

- Section 15 of the PDPA exempts Victoria Police employees from complying with certain IPPs if they believe, at the time of non-compliance and 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.
- The IPPS Victoria Police may be exempt from are outlined in the following table.

IPP	Description
1.3 – 1.5	Information collection; refer to section 1.1 of this policy
2.1	Use and disclosure of information; refer to section 1.2 of this policy
6.1 – 6.8	Access to and correction of information; refer to section 1.6 of this policy
7.1 – 7.4	Unique identifiers; refer to section 1.7 of this policy
9.1	Transborder data flows; refer to section 1.9 of this policy
10.1	Sensitive information; refer to section 1.10 of this policy

- Where possible, Victoria Police should attempt to comply with the IPPs before relying on s.15, PDPA.
- Where s.15, PDPA is relied upon, the employee should create a contemporaneous note that states the reasons why non-compliance with the relevant IPP is necessary.
- Community policing functions under the PDPA are not listed, however, include:
 - licensing investigations
 - location of missing persons
 - providing necessary responses in public emergency and disaster situations and/or
 - locating next of kin, if required.

3.2 *Primacy of other legislation*

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

3.3 *Consent*

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

4. Temporary authorisations

The PDPA contains methods to obtain temporary authorisations for acts or practices that would otherwise breach privacy requirements or, in the case of certification, to provide assurances to facilitate information sharing. These include:

- **Public Interest Determination (PID)** and **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 Victorian Information Commissioner 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.

Employees must engage with the Privacy Unit if they consider they have a requirement to apply for a PID, TPID, IUA or a certification under the PDPA to develop an application and for submission to the Information Commissioner via the Chief Technology Officer. Employees must not contact the Information Commissioner directly.

5. Complaints

- A privacy enquiry is a request for information about how data is collected, used, stored or accessed.
- Employees who receive such enquiries should attempt to resolve the matter directly with the person.
- A privacy complaint is an express concern or dissatisfaction about how data has been handled, including access to data.
- Privacy complaints require a proper investigation. Privacy complaints must be registered with the Privacy Unit. For advice on information privacy complaints or investigations, contact the Privacy Unit. Refer also to **VPM Complaints** for further guidance on complaints and the complaints processes generally.
- Privacy breaches, whether inadvertent or intentional, that have not raised privacy complaints must also be registered with the Privacy Unit.

6. Memorandum of Understanding

- A formal arrangement (such as a Memorandum of Understanding (MOU)) between Victoria Police and external organisations may be used (but is not mandatory) to facilitate appropriate information sharing. To clarify specific processes and ensure the organisations agree to comply with applicable Victorian Protective Data Security Standards (VPDSS) regarding security of law enforcement data, Victoria Police may enter into an MOU with organisations to aid their investigations and functions.
- **VPM Information security** documents the essential requirements for sharing information.
- All MOUs must be developed in accordance with **VPMP Formal arrangements with external organisations**.
- Refer to the Corporate and Formal Arrangements Register or MOU register for access to all current MOUs hosted on the DSSD intranet site.

Related documents

- *Privacy and Data Protection Act 2014*
- *Health Records Act 2001*
- VPM Information security
- VPM Information and records management

Further advice and information

For further advice and assistance regarding these Policy Rules, contact your work unit manager or the Privacy Unit, Digital Services and Security Department via the PRIVACY-OIC PBEA.

Update history

DATE UPDATED	SUMMARY OF CHANGE	FORCE FILE NUMBER
28/01/2026	This VPM updates and replaces VPMG Information privacy.	FF-215906