Office of Public Prosecutions Victoria

OPP Personal and Health Information Privacy Policy

Purpose of this Policy

This policy refers to the use and management of personal and health information collected by the Office of Public Prosecutions (OPP).

All personal and health information held by the OPP is managed in accordance with the privacy principles contained in the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001* and as required by other legislative provisions. The OPP is required by law to have a policy on its information handling practices. As the main role of the OPP is to act under the instruction of the Director of Public Prosecutions (DPP) the DPP adopts the same practices and procedures as the OPP.

Definitions

Personal information is recorded information or an opinion about a living identifiable or easily identifiable individual (including work related information and images).

Sensitive information is information about a living individual's race or ethnicity, political options, religious or philosophical beliefs, sexual preferences or practices, criminal records, or membership details, such as trade union or professional, political or trade associations.

Health information includes information or an opinion about a living or deceased individual's physical, mental or psychological health or disability.

Feedback survey means an online survey offered to people who are victims of crime in cases prosecuted by the OPP, at the end of a case. The OPP uses the Swift Digital Platform for this purpose. More information about Swift Digital and the feedback survey is below.

What does the Office of Public Prosecutions do?

The Office of Public Prosecutions (OPP), led by the Solicitor for Public Prosecutions (SPP), is Victoria's largest criminal legal practice.

The OPP prepares and conducts indictable criminal matters on behalf of the Director of Public Prosecutions (DPP) including:

- Committals in the Magistrates' Court
- Prosecutions in the County Court and Supreme Court
- Appeals in the County Court, Court of Appeal and High Court.

The OPP also provides advice to external agencies, litigates proceeds of crime, and contributes to law reform, on behalf of the DPP.

The OPP briefs Crown Prosecutors, private barristers and OPP solicitor advocates to appear in court on behalf of the DPP.

OPP solicitors and social workers also support victims and witnesses throughout the prosecution process.

The OPP is made up of solicitors, social workers, legal support staff, and corporate and executive services staff who work in different specialist areas.

What areas of the OPP collect personal information?

The OPP receives personal information in relation to offences, defendants, victims and witnesses.

The Human Resources Unit receives personal information including that from staff, from applicants for positions in the OPP, and from statutory office holders connected with the Office.

What does the OPP do with the personal information in receives?

A significant proportion of the personal information handled by the OPP is information it receives from other law enforcement agencies. These agencies collect the personal information in the course of their investigations for the purposes of their respective law enforcement functions or activities. The OPP receives this information in order to assess and prosecute alleged offences, and/or to provide legal advice in relation to the prosecution of offences or the investigation of possible unlawful activity.

The OPP also receives personal information for the purpose of the confiscation of the proceeds of crime and such information may relate to all persons subject to proceedings pursuant to the Confiscation Act 1997. The personal information received is used to prepare legal advice or to prepare documentation or oral evidence for presentation in court.

The non-law enforcement information collected by the OPP is primarily that necessary for the recruitment, remuneration and general management of staff of the Office, former staff or applicants for positions.

What type of personal information does the OPP collect?

The type of personal information the OPP collects or receives consists of a variety of information in relation to its law enforcement function. This may include name, gender, date of birth, address, contact details, relevant personal histories, criminal history, medical histories, financial and asset information relevant to proceedings pursuant to the *Confiscation Act 1997*, fingerprints, licence and motor vehicle registration details, and video evidence from crime scenes. This information may be collected or received in hard copy or electronic format.

The non-law enforcement information collected by the OPP is primarily associated with the management of human resources. It includes information provided by staff – such as names, addresses, next of kin, health information (such as medical certificates), employment histories, qualifications – and information directly and indirectly related to their employment – such as salary, superannuation details, and WorkCover information.

Do any areas of the OPP not have to comply with privacy legislation?

The OPP is required to comply with the Information Privacy Principles (IPPs) and Health Privacy Principles (HPPs) unless it is reasonably necessary not to comply. As the principal role of the OPP is in law enforcement, the OPP is exempt from certain provisions of the IPPs and HPPs when carrying out a law enforcement function and where the OPP believes, on reasonable grounds, that non-compliance is necessary for those functions.

Under the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001*, law enforcement functions or activities include:

- The prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction for a breach; or
- The enforcement of laws relating to the confiscation of the proceeds of crime; or
- Activities in connection with the conduct of proceedings commenced, or about to be commenced in any court or tribunal.

The IPPs and HPPs may also not apply if there is a specific provision in another Act that applies to the handling of information which conflicts with the IPPs and HPPs. If there is a conflict, then the specific provision takes precedence. Similarly, the Office is bound by legal professional privilege and this common law principle will also take precedence over the *Privacy and Data Protection Act 2014* and Health Records Act 2001.

How are the Information Privacy Principles and the Health Privacy Principles applied in OPP?

The *Privacy and Data Protection Act 2014* contains 10 Information Privacy Principles. The *Health Records Act 2001* contains 11 Health Privacy principles of which nine relate to the OPP (as a non-health service provider). The OPP's responsibilities and obligations under both the IPPs and HPPs are adequately captured by the 10 IPPs.

The following is a summary of how these principles are applied in the OPP.

Principle 1 – Collection

It is necessary for the OPP to collect or receive personal information in order to carry out its functions and activities. The OPP will only collect or receive personal information by lawful and fair means which is necessary for its functions. Where the OPP collects or receives personal information for reasons other than law enforcement, persons from whom information is collected will be notified how their information will be used and/or disclosed, and how they can gain access to their information. For law enforcement functions the OPP is exempt from this requirement where it believes on reasonable grounds that the non-compliance is necessary.

Principle 2 – Use and Disclosure

The *Privacy and Data Protection Act 2014* provides that personal information should only be used or disclosed for the primary purpose for which it was collected. However, the Act further provides for use and disclosure for a secondary purpose in certain situations. These include where use and disclosure would be reasonably expected, or if consent has been obtained, or in certain other situations where obtaining consent is not practicable and the individual is not identifiable. The OPP will only use or disclose information for a purpose other than the primary purpose in accordance with the Act and where it believes on reasonable grounds that disclosure is necessary or required by law. This would include the following situations:

- When use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare; or
- When use or disclosure is necessary to lessen or prevent a serious threat to public health, public safety or public welfare; or
- When use or disclosure is required or authorised by or under law; or

- When use or disclosure is reasonably necessary for one or more of the following law enforcement reasons:
    - The prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or
    - The enforcement of laws relating to the confiscation of the proceeds of crime; or
    - The protection of the public revenue; or
    - The prevention, detection, investigation or remedying of seriously improper conduct; or
    - The preparation for or conduct of, proceedings before any court or tribunal, or implementation or the orders of a court or tribunal.

What other practices does the OPP have on use and disclosure of information?

The following reflects OPP policy and practice on the collection and use of specific types of information.

Media

OPP staff observes strict guidelines regarding the type of information that may be disclosed to the media. Personal information including photographs, computer generated images, videos or descriptions may be released if there is a law enforcement purpose for disclosure. However, this is more likely to be done by Victoria Police as part of its community policing activities.

To see what may be disclosed to the media, see the media page on our website.

Electronic Justice System (EJS)

EJS is a system used by a number of law enforcement agencies which is part of the Criminal Justice Enhancement Project (CJEP) Shared Domain systems. It captures some of the information necessary for prosecution and court proceedings.

Data received by the OPP through the CJEP Shared Domain systems is handled in accordance with the *Privacy and Data Protection Act 2014* and the Information Privacy Principles. Employees who need to have access to EJS to perform their duties will be given access with a process of authorisation of users by senior managers. A process of auditing the use of EJS is also provided within EJS which is managed by the Department of Justice.

Authorised users of EJS:

- May access and use EJS information where there is a demonstrable;
- Legitimate business need, which is directly related to the performance of their duties with the OPP;
- Have a public responsibility to protect and keep information they have access to confidential. Information must not be accessed for personal reasons; and
- Are responsible for the security of the information that they access.

Authorised users must treat any information copied, deleted, added, used or disposed of sensitively and professionally with regard to an individuals' right to privacy.

Police Records and Criminal Histories

The OPP obtains and provides criminal history information as required as part of its law enforcement function or where there is a legal requirement to do so. Although the OPP does not create criminal record histories (this is the exclusive responsibility of Victoria Police) the OPP may provide information relating to a prosecution to other government agencies to comply with requests, for example a Working with Children Check.

Unsolicited personal information

From time to time, the OPP receives information from individuals in the form of letters, emails and phone calls that mention other individuals. Such information may refer to another person's welfare or conduct. Where this information relates to law enforcement, the OPP is not obliged to notify the individual that their personal information has been collected if they believe it is reasonable not to in the circumstances.

However, there are occasions where the information received does not relate to law enforcement. On these occasions the OPP will take reasonable steps to notify the individual that their personal information has been collected and what it will be used for.

There may be times where the OPP considers that it is not reasonable to notify the individual of these matters. Even if the OPP does not notify the individual, the information will be protected in accordance with the relevant privacy principles and the OPP policies and guidelines.

Feedback survey

The OPP uses Swift Digital, an online marketing automation platform and service provider to send emails containing links to the online feedback survey, and to collect survey responses at the end of a case.

In using this service, the OPP may collect and use personal information for the purpose of providing access to the online feedback survey, and collecting feedback via the online survey.

All information collected using the Swift Digital service is the property of the OPP and is never shared or used by third parties.

Swift Digital maintains your data in compliance with Australia's *Spam Act 2003* and Australian Privacy Provisions.

All data is maintained within Australia and never leaves Australian jurisdiction. Where stipulated data is encrypted in transit using SSL connections. All data stored via Swift Digital is encrypted at rest.

Principle 3 – Data Quality

The OPP takes reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

Principle 4 – Data Security

Personal information held by the OPP must be protected from misuse, loss, unauthorized access, modification and disclosure. All personal information held by the OPP is kept in a secure environment. Generally, information is destroyed or permanently de-identified when it is no longer required. However, most information is required to be archived in accordance with the *Public Records Act 1973*.

Principle 5 – Openness

The OPP has set out in this Statement how it manages personal information, the nature of the information it holds, the purpose for which it is held and how that information is handled. This Statement is made public via the OPP's website (www.opp.vic.gov.au) or upon request to the FOI Officer of the OPP.

Principle 6 – Access and Correction

Individuals can request access to personal information about themselves held by the OPP. If individuals believe their personal information is inaccurate, incomplete or out of date the individual is entitled to request that it be corrected. There may be circumstances where access to information cannot be granted as it may compromise the privacy of another individual or the exercise of the OPP's law enforcement function.

Section 33 of the *Freedom of Information Act 1982* exempts from release any information which relates to the personal affairs of any person and where release would be unreasonable. There are also other exemptions contained in Part IV of the *Freedom of Information Act 1982* which may apply to exempt a document from disclosure.

All access requests should be sought through the provisions of the *Freedom of Information Act 1982*. You can make an FOI request or find more information about the FOI process by visiting our website opp.vic.gov.au/requesting-advice-or-information/

Principle 7 – Unique Identifiers

Unique identifiers, usually a number, are used by the OPP to enable the organization to carry out its functions efficiently.

Principle 8 – Anonymity

If it is lawful and practicable, a person must have the option of not identifying themselves when entering into transactions with the OPP. However, usually in relation to the OPP's law enforcement function it is necessary for individuals to be identified.

There are many practical reasons why individuals need to identify themselves when interacting with the OPP. For example, for a person to be suitable as a witness it is not possible to be anonymous.

You can visit the OPP website anonymously because the site does not collect or record personal information other than information you choose to provide by email. For further information relating to the way in which you may interact with the OPP's website, refer to the website privacy statement.

Principle 9 – Transborder Data Flows

Pursuant to the *Privacy and Data Protection Act 2014*, an organisation that is transferring personal information to another organisation outside of Victoria must ensure that the receiving organisation has equivalent privacy protection, and that the information transferred will be protected.

Where it is reasonably believed necessary, the OPP is exempt under section 15 of the *Privacy and Data Protection Act 2014* from this obligation in respect of its law enforcement functions and activities. However, precautions related to the security of personal information are undertaken in all trans-border data exchanges by the OPP.

Principle 10 – Sensitive Information

Sensitive information includes information about racial or ethnic origin, political views, religious beliefs, sexual preferences, memberships of groups or criminal record. There are special restrictions on the collection of this information. Where it is reasonably believed necessary, the OPP is exempt from those restrictions where the information is collected for a law enforcement purpose. Otherwise, sensitive information is handled in accordance with the *Privacy and Data Protection Act 2014* which requires the consent of the individual to the collection/use, where the collection/use is required by law or where it is impracticable for the individual's consent to be sought.

How does the OPP handle complaints about privacy?

The OPP has established a complaint handling procedure to deal with any personal information privacy issue that may arise. You can make a complaint or find out more information on the complaints process by visiting our website opp.vic.gov.au/complaints.

Alternatively, if you are dissatisfied with any response, you may contact the Office of the Commissioner for Privacy and Data Protection:

GPO Box 5057
Melbourne Victoria 3001
Telephone: 1300 666 444