ODPP
New South Wales

Privacy Management Plan

October 2023

Contents

Overview

This *Privacy Management Plan* outlines how the Office of the Director of Public Prosecutions (ODPP) ensures it complies with NSW privacy laws when handling personal and health information.

The plan also describes how members of the public can:

- access and amend personal or health information the ODPP may hold about them
- seek a review of ODPP conduct if they believe it breached their privacy.

Purpose

The *Privacy and Personal Information Protection Act* 1998 (PPIP Act) requires the ODPP to develop and implement a privacy management plan that ensures it meets the privacy obligations imposed by that Act and by the *Health Records and Information Privacy Act* 2002 (HRIP Act).

This plan, as required under s33 of the PPIP Act, describes:

- the ODPP's policies and practices to ensure compliance with its privacy obligations
- how officers, Crown Prosecutors and relevant contractors and service providers are made aware of these policies and practices
- the ODPP's procedures for reviewing alleged breaches of its privacy obligations
- other matters relevant to privacy and personal information protection.

Pursuant to s33(4) the ODPP provides a copy of its privacy management plan to the Privacy Commissioner, as soon as practicable after it is amended.

Consistent with the Information and Privacy Commission's *Guide to making privacy management plans* (*the Guide*), this plan also describes:

- the ODPP's key functions and activities
- the main kinds of personal information and health information it handles.

Definitions

Personal information	Information or an opinion about an individual 'whose identity is apparent or can reasonably be ascertained from the information or opinion' (see *s4 PPIP Act*). Personal information can include a person's name, address, information about their family life, information about their sexual preferences, financial information, video or audio footage, fingerprints, retina prints, blood or DNA samples. Section 4(3) of the PPIP Act lists information that is not 'personal information' (which includes information that is publicly available).
Health information	Information or an opinion about a person's physical or mental health or disability, their wishes about future provision of a health service to them, or a health service provided, or to be provided, to them (see *s6 HRIP Act*).
Collection	How the ODPP acquires personal information or health information, which can include from a brief of evidence, written document, email, verbal conversation, a voice recording, CCTV, or a video / photograph. NB: Personal information / health information is not 'collected' if unsolicited (*see s4(5) PPIP Act*, *s10 HRIP Act*).
Disclosure	When the ODPP makes known personal information or health information to an individual or entity that was not previously in possession of that information.
Privacy principles	The Information Protection Principles set out in Division 1 of Part 2 of the *PPIP Act* and the Health Privacy Principles set out in Schedule 1 of the HRIP Act. These principles establish the minimum standards for all NSW public sector agencies when handling personal information and health information.

About the ODPP

The ODPP's key function is to prosecute serious crimes in NSW on behalf of the community. It handles close to 18,000 matters a year involving offences under the laws of the State.

As a prosecutor, the ODPP is entrusted with a great deal of sensitive and confidential information related to victims, witnesses, accused and others.

As a public sector employer and an administrator of public resources, the ODPP is entrusted with sensitive information about officers, Crown Prosecutors, contractors and service providers.

Policies and practices to ensure compliance

The ODPP has policies and practices in place to address the key areas of compliance under the *PPIP Act* and the *HRIP Act*, which the *Guid*e lists as:

- the personal information and health information handled
- the Information Protection Principles under the *PPIP Act* and Health Privacy Principles under the *HRIP Act* (the Privacy principles)
- relevant exemptions in the *PPIP Act* and the *HRIP Act*
- offences under the *PPIP Act* and the *HRIP Act*.

To ensure its policies and practices continue to address its privacy obligations, the ODPP also:

- examines changes in the legislative, policy and/or operational environment to identify impacts on privacy management
- implements the privacy related policies and procedures developed for the NSW public sector as a whole
- considers the privacy implications of changes to policies and systems.

Personal and health information the ODPP collects

Table A: Information the ODPP collects as a prosecutor, employer and administrator

Personal and health information the ODPP collects as a prosecutor	Personal and health information the ODPP collects as an employer / administrator
To perform its prosecution function, the ODPP collects personal and health information in briefs of evidence submitted by the following investigative agencies: • NSW Police Force • Law Enforcement Conduct Commission • NSW Crime Commission and • Independent Commission Against Corruption. • Australian Federal Police These briefs of evidence are in either hard copy or electronic format or a combination of both. While preparing and prosecuting matters, the ODPP also collects additional personal and health information from these investigative agencies and from other sources: particularly from witnesses, victims of alleged offences and their families, other government agencies, legal representatives acting for defendants and accused persons and members of the public. Such information is in both hard copy and electronic format. It is received via post, hand delivery, email, phone, during face to face interactions and via Audio Visual Link (AVL) interactions. Examples include transcripts of proceedings and expert medical evidence; Notices under the Evidence Act, Alibi Notices and subpoenas for production of documents from legal representatives; Victim Impact Statements from victims of crime and members of their families.	As an employer and administrator of public resources, the ODPP collects personal and health information related to the recruitment, employment and performance of ODPP officers, the recrutitment and appointment of Crown Prosecutors, the engagement and performance of services by its contractors and service providers and the procurement of goods and services. This information includes: • contact details • resumes including qualifications and employment history • references • citizenship / residency checks • criminal history • Working With Children checks • professional development and education • performance • secondary employment • conflicts of interest • next of kin and their contact details • family and care arrangements • financial information (such as tax file numbers, banking details, superannuation fund details, salary deductions, salary history, garnishee orders) • leave including flex, recreation, sick, study and special leave related records • workers' compensation related records • vaccination status information. Much of the above information is collected by email and at interview during the recruitment and employment / engagement process. Further information of this kind is collected and received

	during an officer's period of employment or a contractor's period of engagement.

As a prosecutor, employer and administrator, the ODPP also:

- records and retains for a period, CCTV footage of some activities within the ODPP's office premises, for security purposes
- requires police checks for individuals seeking to enter the ODPP's office premises to provide services, such as tradespeople and cleaners
- collects personal information from visitors to the ODPP's office premises (such as name, organisation, contact details, vaccination status, time and date of visit and reason for visit) for OHS and security purposes
- handles requests for information under the *Government Information (Public Access) Act* 2009 (the *GIPA Act*).

The Office does not maintain a public register that contain personal or health information.

Compliance with the privacy principles

The 12 Information Protection Principles set out in the PPIP Act and the 16 Health Privacy Principles set out in the *HRIP Act* (the Privacy principles) constitute privacy standards and impose obligations on the ODPP relating to the collection, retention and security, access to and amendment of, use, and disclosure of personal information and health information.

The ODPP's strategies for complying with the Privacy principles, examples of compliance, and the relevant exemptions from compliance are set out in Table B, which begins on page 8.

The PPIP Act provides multiple exemptions from the Information Protection Principles for law enforcement agencies, which includes the ODPP (see s3). The PPIP Act provides further exemptions for agencies when carrying out law enforcement functions, and exemptions of more general application. The *HRIP Act* also provides exemptions for law enforcement and other activities relevant to the ODPP.

Together, these exemptions apply to a significant number of the ODPP's activities as a **prosecutor**. For this reason, while this plan covers all ODPP activities, the Privacy principles and the compliance strategies outlined in Table B are of most relevance to the ODPP's functions as an **employer** and **administrator**.

Shading in Table B denotes that exemptions common to multiple Privacy principles apply.

Table B: ODPP Compliance with the Information Protection Principles and the Health Privacy Principles

The Privacy principles and how the ODPP complies with them (Shading indicates that exemptions from the Information Protection Principles that are common to multiple Principles apply. These general exemptions are listed at the end of the table, on p 15. Exemptions specific to a Principle are included in the table.)	Privacy principle
Collection	*The ODPP collects personal and health information only for lawful purposes directly related to a function or activity and when collection is reasonably necessary for that purpose.* *It collects information by lawful means only.*	IPP1, Section 8 PPIP Act, Principle 1 Sch 1, HRIP Act
	For example: • the ODPP requires individuals seeking employment or promotion to provide only the information that is relevant to their suitability and eligibility to perform the role.	

	The ODPP collects information about an individual directly from the individual unless:
	• *for personal information,*
	  ○ *collection is otherwise authorised by the individual or*
	  ○ *if the individual is under 16 years old, the information is provided by a parent or guardian*
	• *for health information, collection from the individual is unreasonable or impracticable.*
	Health information is collected according to guidelines issued by the Privacy Commissioner.
		IPP2,Section 9 PIPP Act, Principle 3 Sch 1 HRIP Act

	In addition to the exemptions from the Information Protection Principles outlined at the end of this table, exemptions apply to the collection of *personal* information: • if compliance would prejudice the ODPP's law enforcement functions (s23(1)) or the individual's interests (s26(1)) • when information is collected in connection with court or tribunal proceedings. (s23(2))	
	An example of a relevant ODPP practice is: • when an officer member has transferred to the ODPP from another government department and the ODPP receives information on their employment and salary history from that department, the ODPP assumes, as is the usual practice in	

the public sector, that this information was initially collected from the individual concerned or collected pursuant to their prior authorisation.

IPP 3, Section 10 PIPP Act, Principle 4 Sch 1 HRIP Act

The ODPP does not collect information from an individual without making it clear to them:

- *that the information is being collected, and why*
- *who will receive the information*
- *whether the supply of the information is voluntary or required under law, and any consequences if it isn't provided*
- *any right they have to access and correct the information*
- *the ODPP's identity and contact details.*

In addition to the exemptions from the Information Protection Principles outlined at the end of this table, exemptions apply to both *personal* and *health* information when:

- the individual consents (s26(2), P4(4)(a))
- information is collected for law enforcement purposes (s23(3), P4(4)(e))
- compliance would prejudice the individual's interests (s26(1) (P4(4)(d)
- a public sector agency or public sector official is investigating or handling a complaint or other matter that could be referred to an investigative agency (P4(7)).

Examples of ODPP's compliance include:

- providing officers with information on the purpose of the NSW Workforce Profile Data Collection and advising that they can have their information excluded from the data collected
- when inviting officers to participate in the 'People Matter' NSW public sector survey, advising them of the reason the survey is conducted, how the information collected will be used, and the steps taken to ensure anonymity and confidentiality
- advising officer's of the ODPP's policy of confirming service and salary details when approached by financial institutions

- advising officers asked to participate in an investigation into another officer's conduct that their identity and what they say will be included in the investigation report, which will be provided to the officer whose conduct is being investigated
- making clear in IM&T user registration forms and the Information Security Policy that officer's access to and use of ODPP information technology systems is monitored and recorded, and the reasons for this
- installing signs on the walls of ODPP office premises to advise officers and visitors if CCTV is operating.

The ODPP only collects information that is relevant to its functions. In doing so, it takes steps to collect up-to-date, necessary, accurate and complete information, and takes care not to be unreasonably intrusive.

IPP 4, Section 11 PIPP Act, Principle 2, Sch 1, HRIP Act

Examples of compliance include:

- when supporting victims of crime, only seeking the information necessary to provide an appropriate support service
- where appropriate, requiring officers and contractors to check and verify the accuracy of the information the ODPP has collected about them.

Storage

The ODPP has information handling and security policies and procedures in place to safeguard against loss, unauthorised access, use, modification or disclosure of the information it collects. These policies and procedures also ensure the information is retained for no longer than is necessary for the purposes for which the information may lawfully be used, and disposed of appropriately, including by archiving. The ODPP also seeks to ensure that, if it is necessary for information to be given to a person in connection with the provision of a service to the ODPP, it takes reasonable steps to prevent unauthorised use or disclosure of the information.

IPP5, Section 12 PIPP Act, Principle 5, Sch 1, HRIP Act

The relevant policies include the ODPP's:

- *Information Classification, Labelling and Handling Policy*, which establishes information storage, dissemination and disposal standards for sensitive information, in both digital and physical form
- *Information Security Policy*, which ensures the security, integrity and accessibility of the information created, shared and stored on our digital network and that information and communications technology use is consistent with the ODPP Signature Behaviours, Code of Conduct, policies and procedures, legislative requirements and Public Sector obligations including:
    - new users required to sign confidentiality and 'terms and conditions for use' agreements before gaining access

	○ privileges assigned based on roles ○ all ODPP digital systems password protected using secure / complex passwords ○ all user activity that may affect information security tracked ○ use in breach of any State or Commonwealth law forbidden • *Cloud Services Policy* which provides that when considering cloud-based services the decision on the appropriate delivery model will be based on whether the solution provides adequate risk management and adequately considers all relevant factors under the NSW Government Cloud Policy. • the *Code of Conduct*, which: ○ requires compliance with relevant federal and state legislation (including privacy legislation), whole of government policies and directives, and all internal policies, procedures, guidelines and work instructions ○ requires respect for individuals' privacy, confidentiality and values ○ includes standards to ensure confidentiality of physical and digital information ○ requires reporting of unethical, corrupt or criminal conduct • the *Social Media Policy,* which establishes a responsibility not to harm the discharge of any ODPP function, the professional or personal lives of colleagues, or the reputation or operations of stakeholders. • The *Data Breach Policy,* which provides guidance on how to identify and respond to a data breach and ensures compliance with mandatory reporting schemes.	
Access	See *Information access, alteration and review* on page 21 for the rights of individuals to access and amend the information the ODPP holds about them, and the exemptions that apply.	IPP 6-8 Sections 13–15, PIPP Act, Principles 6–8 Sch 1, HRIP Act
Use	*The ODPP does not use information it holds without taking reasonable steps to ensure it is relevant, accurate, up-to-date and complete.* **Examples** of compliance include:	IPP 9, Section 16 PIPP Act, Principle 9,

- not providing a background report on an accused person when requested to do so by another agency conducting later proceedings, if the report is no longer current or otherwise no longer relevant
- regularly reminding officers to update on SAP the information the ODPP holds about them
- requiring IT users to submit a registration every time they relocate or transfer to a new role.

Sch 1, HRIP Act

The ODPP does not use information other than for the purpose for which it was collected unless:

- *the individual consents or*
- *the other purpose is directly related to the collection purpose or*
- *doing so is necessary to prevent or lessen a serious and imminent threat to the life or health of the relevant individual..*

IPP 10, Section 17 PIPP Act, Principle 10 Sch 1, HRIP Act

In addition to the exemptions from the Information Protection Principles outlined at the end of this table, exemptions apply to the use of:

- *personal* and *health i*nformation, when
  - reasonably necessary for law enforcement purposes (s23(4), P10(1)(j))
  - disclosure is to another public sector agency under the same Minister to inform the Minister about a matter within that Minister's administration (s28(3)(a), P10(4)(a))
- *personal* information, when use is necessary to protect the public revenue (s23(4)
- *health* information, if the ODPP has reasonable grounds to suspect unlawful activity or misconduct and the use is necessary for investigation or reporting purposes. (P10(1)(h))

Examples of compliance include:

- the personal information the ODPP collects when recruiting is used only for the purposes that an officer would expect – such as setting up payroll and personnel files for the officer
- the ODPP does not extract information from its case management system about an individual for use in a later unrelated proceeding unless reasonably necessary for law enforcement purposes.

Disclosure

The ODPP does not disclose the information it collects about an individual unless:

- *the individual consents (s26(2); P11(1)(a))*

IPP 11, Section 18 PIPP Act,

- *the disclosure is directly related to the purpose for which the information was collected and the ODPP has no reason to believe the individual would object*
- *the individual is likely to be aware that that type of information is usually disclosed to another person or organisation*
- *disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another person..*

Principle 11, Sch 1, HRIP Act

In addition to the exemptions from the Information Protection Principles outlined at the end of this table, exemptions apply to the disclosure of:

personal and *health* information:

- made in connection with proceedings for an offence or for law enforcement purposes (s23(5)(a), P11(j))
- in order to investigate an offence when there are reasonable grounds to believe that an offence may have been committed (s23(5)(d)(ii), P11(1)(i))
- to another public sector agency under the same Minister, to inform the Minister about a matter within that administration (s28(3)(a), P11(4))

personal information when disclosure is:

- reasonably necessary to assist an investigative agency exercising an investigative function (s24(4))
- to a law enforcement agency for the purposes of finding a missing person (s23(5)(b))
- authorised or required by subpoena, search warrant, or another statutory instrument (s23(5)(c))
- reasonably necessary to protect the public revenue (s23(5)(d)) and s23(8)
- requested by the Director General of ASIO s23A (2),(3)

health information

- disclosed while investigating unsatisfactory professional conduct or conduct that may be grounds for disciplinary action. (P11(1)(i))

Examples of where the ODPP would not disclose health information while performing its function as a prosecutor are:

-to a victim, when ODPP receives information about an accused person's health ahead of a trial or sentencing – for example, the ODPP would not disclose to a victim that an accused had been diagnosed with severe dementia but would instead

inform them that the accused's health is likely to be an issue in proceedings, and ODPP would then wait for further details to be put on the public record relating to the accused's health

-the ODPP does not provide NSW Police with reports / documents related to the mental health of a defendant who is a police officer, tendered in summary proceedings where a magistrate has been asked to make an order under s14 of the *Mental Health and Cognitive Impairment Forensic Provisions Act 2020*.

An example of where the ODPP would disclose:

- personal information is
    - to another public sector agency proposing to make an officer an offer of appointment. This 'services check' is common practice throughout the public sector and it is considered that s18(1) of PPIP Act applies

health information is

- to a health practitioner, for example, an ambulance officer, if an officer had a health emergency at work and the ODPP held information about that officer that could assist in their immediate treatment and care.

Other examples of disclosure practices

Under s11 of the *Independent Commission Against Corruption Act*, the Director has a duty to report to the Independent Commission Against Corruption any matter which, on reasonable grounds, the Director believes concerns or may concern corrupt conduct. Section 25 of the PPIP Act provides that a public sector agency is not obliged to comply with section 18 if the agency is lawfully authorised or required not to comply with the relevant Principle. Health Privacy Principle 11(2) is to the same effect in relation to the disclosure of health information.

The ODPP has an established procedure agreed with NSW Police, under which allegations of suspicious or corrupt conduct by police officers are reported directly to the appropriate agency.

If the NSW Police or a public sector agency seek a copy of a brief or another document to investigate a disciplinary offence allegedly committed by an employee, the ODPP will only provide information that is publicly available, unless ODPP receives a subpoena for production or a compulsory direction to produce documents. The ODPP's Privacy Officer provides advice, where required, in this situation.

In appropriate circumstances the ODPP will report unethical behaviour by lawyers to the Legal Services Commissioner.

The ODPP's Witness Assistance Service (WAS) officers, when referring clients to specialist services, will only disclose the personal or health information to which the client has given consent.

When performing its function as a prosecutor, the ODPP will sometimes prevent disclosure of information relating to a child to their parent, when the child does not want the information to be provided. In these cases, officers assess the circumstances of the child and their relationship with the person seeking the information (for example, a non-offending parent) before making a decision.

The ODPP has a *Public Interest Disclosures policy* for internal reporting under the *Protected Disclosures Act* 1994.

When disclosure of sensitive personal or health information is necessary, the ODPP labels it 'Sensitive: Personal' as an additional layer of protection, as required under its *Information Classification, Labelling and Handling Policy*.

Research: The ODPP only provides access to its files for academic research purposes when the researcher has complied with the Privacy Commission's relevant direction, which requires an ethics committee to have approved the research project. Section 27B of the PPIP Act contains detailed provisions relating to research and the compilation or analysis of statistics in the public interest, with which the ODPPP complies. Health Privacy Principles 10 and 11 contain specific provisions relating to the use and disclosure of health information for research or the compilation or analysis of statistics: see Principle 10(1)(f) and Principle 11(1)(f, with which the ODPP complies.

Media: The ODPP only releases information to the media that is on the public record or otherwise authorized by the Director: for example a Director's press release relating to the Director's decision not to further pursue criminal proceedings in a particular matter.

Data Breach: The ODPP has a *Data Breach Policy* which provides guidance to staff in circumstances where there is unauthorised disclosure of personal or health information, for example as a result of a cyber attack or accident. The Policy provides that the ODPP will notify, affected parties when required and the Privacy Commissioner of any breach.

The ODPP complies with the strict requirements in the PPIP Act not to disclose information on an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person..

The ODPP does not disclose personal or health information outside of NSW unless the individual to whom it relates expressly consents, or the recipient is subject to privacy obligations which are similar to the privacy obligations that apply to the ODPP. The ODPP also has regard to the detailed list of exemptions in section 19(2) when considering requests for information from agencies/individuals outside NSW and from a Commonwealth agency.

IPP 12, Section 19(1) and 19(2) PIPP Act Principle 14, Sch 1, HRIP Act

In addition to the exemptions from the Information Protection Principles outlined at the end of this table, exemptions apply to *personal* information:

- for law enforcement purposes where there are reasonable grounds to believe an offence may be, or may have been, committed (s23(7))
- when disclosure is to another public sector agency under the same Minister to inform the Minister about a matter within the administration (s28(3)(a)
- to an investigative agency that is exercising its investigative functions s24(4)
- if the individual to whom the information relates would benefit from the disclosure and has expressly consented to the disclosure s26 (2)

Examples of compliance include:

- The ODPP is sometimes asked for information by government agencies outside of NSW, such as interstate prosecution agencies or police services prosecuting / investigating a person the NSW ODPP has previously prosecuted. The ODPP requires that these requests be made formally and include the purpose for which the information is being sought. The ODPP provides the information requested only where it considers the requesting agency has a legitimate interest in acquiring it, or the individual expressly consents.
- The ODPP does not assign identifiers to individuals or disclose any identifiers that are assigned unless necessary to perform its functions. As an example of disclosure, when relevant the ODPP will nominate a role within the organisation as having to be filled by an individual who identifies as Aboriginal or Torres Strait Islander. (s19, p12)

Exemptions from multiple principles when the ODPP is handling *personal* information (represented in Table B above by shading)

The ODPP is not required to comply with the Information Protection Principles for the collection, use or disclosure of ***personal*** **information:**

- when the information is being provided to or by another public sector agency and is reasonably necessary
    - for law enforcement purposes (23(6A)(b))
    - to deal with correspondence from a Minister or Member of Parliament (s27A(b)(i))
    - to refer inquiries between agencies (s27A(b)(ii))
    - for auditing accounts or performance (s27A(b)(iii))
- when necessary for research or to compile or analyse statistics when in the public interest (s27B(a)) and it is unreasonable or impractical to collect the information from the individual (s27B(b)).
- when necessary to assist in a stage of an emergency (s27D (1))
- non compliance is lawfully authorised or required (s25)

The above exemptions for **use** and **disclosure** for research or statistical purposes only apply if the research purposes can't be served without using or disclosing identifying information and the individual's consent can't be practically obtained (s27(B)(c)(i)), or steps are taken to de-identify the information (s27B(c)(ii)). If disclosure could identify individuals, information cannot be published in a publicly accessible way (27B(d).

Offences under privacy legislation

Under both the *PPIP Act* and the *HRIP Act*, it an offence for the ODPP to:

- intentionally disclose or use personal or health information accessed while performing an official function for an unauthorised purpose
- offer to supply personal or health information that has been disclosed unlawfully.

It is also an offence under:

- the *PPIP Act*, to hinder the Privacy Commissioner or a staff member from doing their job
- the *HRIP Act*,
    - to attempt to persuade an individual not to make, or to withdraw, an application for a request for access to health information or a complaint to the Privacy Commissioner or Tribunal
    - by threat, intimidation, or false representation, to require another person to give consent or to do, without consent, an act for which consent is required.

The ODPP minimises the risk of a privacy offence occurring through its privacy awareness training (see *Raising awareness of privacy obligations* below) and by requiring the highest standards of ethical conduct from everyone who performs work for it. It has developed Signature Behaviours, which include acting with integrity, as a key aspect of its Strategic Plan and a component of officer's performance development. These Signature Behaviours in turn form part of the ODPP *Code of Conduct*, which establishes ethical principles and standards of conduct for all decisions made and action taken on the organisation's behalf, and all behaviour while performing work for it. The Code and relevant policies specifically require compliance with the PPIP Act and the HRIP Act. The Code also requires individuals to report conduct that is unethical, corrupt, serious misconduct, or criminal.

All staff employed under the *Government Sector Employment Act 2013* (*GSE Act*) are also legally obliged to comply with the *Ethical Framework for the government sector*, which is established by Part 2 of the Act. The *Code of Conduct* extends this obligation to all individuals performing work for the ODPP.

Raising awareness of privacy obligations

Internal awareness and promotion

To ensure ODPP officers, Crown Prosecutors, contractors and service providers are aware of and understand their privacy obligations and how they apply to the work they do:

- the ODPP's **executive team**
  - appoints privacy officers (the Deputy Solicitor, (Legal)) and Deputy Solicitor (Legal Operations)
  - reviews and endorses the Privacy Management Plan, after it is periodically updated
  - identifies and takes into account privacy issues when implementing new systems and other changes

- the **Deputy Solicitor, (Legal), Deputy Solicitor (Legal Operations)** and the **Director, Human Resources** ensure:
  - this Privacy Management Plan is published in a prominent place on the intranet
  - the plan and an overview of the PPIP Act and the HRIP Act are included in induction packs for officers and, where relevant, provided to contractors
  - privacy obligations are addressed in induction programs and in training refresher courses
  - officers and contractors are aware that the Deputy Solicitor (Legal) and Deputy Solicitor (Legal Operations), are the ODPP's Privacy Officers and should be contacted for information / advice
  - officers and contractors are notified via the intranet of any relevant changes to the ODPP's privacy obligations
  - the ODPP's privacy obligations are highlighted at least once a year (for example, during Privacy Awareness Week)
  - policies and other documents, where relevant, specifically require compliance with privacy legislation

- **managers** are required to ensure that officers within their area of responsibility, who handle personal or health information are aware of their specific privacy obligations.

- All staff are required to attended privacy training during their induction and complete a privacy awareness online learning module. Staff should report any suspected privacy breaches or other privacy related concerns to the Privacy Officers.

Public awareness and promotion

To ensure members of the public understand how the ODPP meets its privacy obligations, this plan is easily accessible on the organisation's website (odpp.nsw.gov.au).

The ODPP also:

- provides print copies of the plan free of charge on request
- informs members of the public who contact the organisation with a privacy question or concern about this plan and
- that the ODPP has a Privacy Officer.

Information access and alteration (Privacy principles sections 13–15 PPIP Act, Principles 6–8 HRIP Act)

Right to access and amend information

ODPP staff, Crown Prosecutors, contractors, service providers and members of the public are entitled to:

- find out whether the ODPP holds personal or health information about them and if it does, the nature of the information and how it is used (s13 PPIP Act; Health Privacy Principle 6(1)(c))
- access that personal and / or health information held about them (s14 PPIP Act; Health Privacy Principle 7))
- seek amendments to that information if it is incorrect, inaccurate, incomplete, misleading or irrelevant (having regard to the purpose for which the information was collected or is to be used (s15 PPIP Act; Health Privacy Principle 8).

Requests for information, access and amendments should be made in writing to the Privacy Officers (the Deputy Solicitor, (Legal)) and Deputy Solicitor (Legal Operations).

ODPP is exempt from the obligation to apply these principles when:

- the ODPP is lawfully authorised or required not to comply (s25(a), (p6–8(2)(a)) and Health Privacy Principles 6(2); 7(2); and 8(4). See also the section relating to the *GIPA Act* later in this section of the plan
- non-compliance is otherwise permitted under law (s25(b), p6–8(2)(b) and Health Privacy Principles 6(2); 7(2) and 8(4).).
- the information which is the subject of the request is covered by the ODPP"s Code of Practice under Part 3 of the Privacy Act (refer to next section for details)
- compliance with the request would reveal to the public that ASIO had requested or been provided with, information about a person (s23A(1))

Government Information (Public Access) Act 2009 (GIPA Act)

Applications under the GIPA Act for prosecution files or any information contained within such files, are invalid because prosecution information is excluded information under the GIPA Act. The ODPP will not provide this information if it is requested pursuant to the Act. However, the ODPP exercises some discretion in relation to its release of information from a police brief or a prosecution file, where the information is requested by the person to whom it relates: for

example, upon request, the ODPP will provide to a prosecution witness, a copy of their police statement and any health information held about them.

How to access and amend information

Officers and Crown Prosecutors: Officers and Crown Prosecutors can view the information the ODPP holds about them through the PATH portal and can amend most of this information themselves. However, some PATH information changes, such as name changes, require documentary evidence and need to be requested through Human Resource.

Contractors, Service Providers and Members of the public: If you are a contractor, service provider or member of the public seeking to access personal / health information, you don't have to make a formal application. As a first step, you can make enquiries directly by phone or email (see Appendix A: *ODPP contact details for privacy questions / concerns).*

If the ODPP does hold information about you and it is inaccurate, out of date or incomplete, you can request changes, again, without making a formal application (although sometimes verifying documents will be required). The ODPP will attempt to deal with an informal request for change within five working days of receiving it, and will advise you of the outcome.

In some cases, particularly if the information you seek to access and / or amend is sensitive, the ODPP will ask you to make a **formal application**. You can also submit a formal application as a first step if you prefer, or if you are not satisfied with the outcome of a less formal request. Formal applications must be in writing and should:

- include your name and contact details, including your postal address, phone number and email address
- indicate whether you are making the application under the PPIP Act (for personal information) or the HRIP Act (for health information)
- explain what personal or health information you want to access or amend, and the changes you are seeking.

Formal applications are dealt with by the ODPP's Privacy Officers, who will seek to respond to you in writing within 20 working days.

If the ODPP is not prepared to make your proposed amendments, you can provide a statement about the changes you sought, and your statement will be attached to the information held about you.

Internal and External Review (Part 5 PPIP Act)

Right to internal review

Any person who believes the ODPP has breached its privacy obligations to them has a right, under s53 of the PPIP Act, to an internal review of the alleged breach.

An application for a review must be in writing (a form is available at odpp.nsw.gov.au) and made within six months of you becoming aware of the alleged breach. The ODPP may consider late applications, depending on the circumstances.

Once you have filled out the application form, email or post it to the ODPP Privacy Officer, or hand it to reception at the ODPP office nearest to you (see Appendix A).

The ODPP will aim to:

- acknowledge receipt of the formal application within **five working days**
- complete the review within **60 calendar days.**

If you think your concerns can be resolved quickly and easily, contact the ODPP to discuss your concerns, before you apply for a formal review. You will be put in contact with a Privacy Officer, who can explain the ODPP's obligations to you and whether it appears they have been breached. You can also discuss whether and if so, how, the ODPP can address your concerns. This discussion may help you to decide whether to proceed with a formal application for internal review.

You are also entitled to make a direct complaint to the Privacy Commissioner about an alleged breach of your privacy by the ODPP: sections 45-51 PPIP Act; without applying to the ODPP for an internal review.

Review process

The key questions the ODPP's Privacy Officers will examine in a review of an alleged breach are:

- whether the alleged breach occurred ie whether the conduct alleged to have breached the Privacy principles, in fact occurred
- if so, whether that conduct was a breach of the ODPP's privacy obligations
- whether any exemptions from the ODPP's privacy obligations apply to the particular circumstances.

The Privacy Officers will follow the Privacy Commissioner's guidance, including 'How to handle an internal review' and the 'Privacy internal review checklist', when conducting the review.

Privacy Commissioner's role in internal reviews

The ODPP must notify the Privacy Commissioner when it is conducting an internal review and inform it of the progress of the review, and the findings and proposed action.

The Privacy Commissioner is entitled to make submissions to the ODPP about the matter.

The Information and Privacy Commission can be contacted on 1800 472 679 or via ipcinfo@ipc.nsw.gov.au

Review outcomes

Possible outcomes of an internal review include that the ODPP:

- takes no further action
- apologises to you
- takes appropriate action to remedy the breach (this could include financial compensation under the privacy legislation)
- provides undertakings that the conduct will not occur again
- implements measures to ensure that the conduct will not occur again.

The ODPP will inform you of the outcome of its internal review as soon as possible, and within **14 days** of a decision being made.

If you are not satisfied with the outcome of the internal review or are not notified of it within **60 calendar days**, you have the right to seek an **external review** of the alleged breach (see below).

External reviews

External reviews of alleged privacy breaches are conducted by the NSW Civil and Administrative Tribunal (NCAT). NCAT can make orders, including damages awards under the privacy legislation, to remedy the conduct if satisfied it caused you financial loss, or psychological or physical harm.

You have 28 days from the date of being notified of the internal review decision to seek an external review. To do so, you must apply directly to NCAT. Details are available at https://www.ncat.nsw.gov.au, or you can call 1300 006 228, or visit Level 9, John Maddison Tower, 86–90 Goulburn Street, Sydney NSW 2000.

Reporting on reviews

The ODPP reports on requests for, and outcomes of, internal reviews and external reviews of privacy related conduct in its annual reports.

Review of management plan

The ODPP will review this privacy management plan every two years, and earlier if necessary as a result of relevant legislative, administrative or systemic changes.

Document ownership, control and history

Version	Owner	Approved by	Approved by Director
1	E.Kwiet	C. Hyland	7 August 2023

Appendix A: ODPP contact details for privacy questions / concerns

The ODPP's Privacy Officer can answer questions about this plan and about the personal and health information the ODPP holds about officers, Crown Prosecutors, contractors, service providers and members of the public.

To contact the Privacy Officer, or to submit a formal application for an internal review of an alleged breach by the ODPP of its privacy obligations:

Email	enquiries@odpp.nsw.gov.au (include 'Privacy' in the 'Subject' field)
Phone	1800 814 534 (toll free) and ask to speak to the Privacy Officer
Mail	ODPP Privacy Officer Locked Bag A8 Sydney South NSW 1232
Visit	See the Contact us page of the ODPP's website for the location and phone numbers of its offices throughout NSW.

ODPP
New South Wales

Office of the Director of Public Prosecutions

Level 17, 175 Liverpool Street
Sydney NSW 2000
Locked Bag A8
Sydney South NSW 1232
DX 11525 Sydney Downtown

Phone 02 9285 8606
Fax 02 9285 8600
TTY 02 9285 8646

odpp.nsw.gov.au