Privacy Management Plan

Legal Branch, Office of General Counsel

April 2022

NSW GOVERNMENT Premier & Cabinet

Document management

Author:	Director, Information and Privacy Legal Branch
Revision history:	Version No. 1 (2000) Version No. 2 (2012) Version No. 3 (February 2015) Version No. 4 (May 2015) Version No. 5 (September 2019) Version No. 6 (April 2022)
Next review date:	April 2024
Responsible Branch:	Information Access and Privacy Unit, Legal Branch

Copyright

Disclaimer

Contents

1. About this Privacy Management Plan

1.1 Purpose

Section 33 of the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) requires each public sector agency to have a privacy management plan.

This Plan covers the NSW Department of Premier and Cabinet (**Department**).

The purpose of this Privacy Management Plan (**Plan**) is:

- to demonstrate to members of the public how the Department upholds and respects the privacy of its clients, staff and others about whom the Department holds personal information, and
- to act as a reference tool for the Department's staff, to explain how they can meet their privacy obligations under the PPIP Act and the *Health Records and Information Privacy Act 2002* (NSW) (**HRIP Act**).

1.2 History of the Plan

The Department's first Privacy Management Plan was drafted in 2000. A comprehensive review of the Department's privacy functions was undertaken in 2018 and 2019 and resulted in a number of improvements being made, including:

- updating and expanding internal training materials on The Hub and learning management system,
- adopting a risk-based approach to privacy management resulting in updates to relevant precedent materials (including procurement documentation),
- expanding the material included in the Plan to provide access to a broader suite of material dealing with best-practice privacy management, and
- updating the Plan to reflect current legislative and policy frameworks.

As set out in section 33(4) of the PPIP Act, the Department may amend the Plan from time to time. Given the nature and extent of personal information typically collected by the Department, we aim to review the Plan every two years. The next review date is set out in the 'Document Management' section at the start of the Plan.

2. Promoting the Plan

We employ the following broad strategies to ensure ongoing compliance with privacy legislation:

- as part of our induction program, new staff are provided with information to raise their awareness and appreciation of the privacy legislation requirements,
- we provide refresher and on-the-job training for specialist staff,
- we highlight and promote the Privacy Management Plan during the annual Privacy Awareness Week/Month,
- where we propose to collect personal information through forms, questionnaires, survey templates, interview sheets etc, the relevant documents are reviewed by the responsible managers to ensure compliance with privacy principles,
- when existing tools for collecting personal information are updated, managers review them to ensure compliance with privacy principles,

- we provide specialist advice internally to staff, relating to the interpretation and practical implementation of the privacy legislation,
- the Plan is published on our website,
- the Plan is desktop reviewed and updated every two years, and
- every five years we formally and comprehensively review/audit our compliance with the privacy legislation, including a review of the governance framework and controls in place to manage privacy within the Department, which includes the Plan (the next audit is due to be undertaken by December 2023).

3. The Department

The Department is the lead central agency in the NSW Government. It supports the Premier, the Cabinet, Ministers and agencies by coordinating policies and services and delivering priority projects.

The Department:

- provides leadership in policy development through its statutory and strategic role,
- provides advice and innovative ideas,
- coordinates and supports Government plans and projects,
- provides support to agencies to achieve policy and service delivery reform,
- negotiates the resolution of issues, and
- coordinates the initiatives of Ministers and their agencies to achieve targets and works with the Federal Government to fulfil other commitments.

Further information can be found on the Department's website.

4. Privacy obligations

The Department collects, holds, uses and discloses personal information (including health information) for the purpose of carrying out its functions. For instance, the Department may handle personal information for the purpose of managing correspondence on behalf of the Premier and for coordinating significant events. The Department is regulated by the PPIP Act and the HRIP Act.

Note that health information is a particular type of personal information, as defined in the HRIP Act. The Department does not have a separate privacy management plan for health information. References in this Plan to personal information should be taken to include health information, but where relevant, any special provisions that apply to health information will be set out.

4.1 Privacy principles

Both the PPIP Act and HRIP Act prescribe 'privacy principles'. The PPIP Act covers personal information other than health information and requires agencies to comply with 12 information protection principles (**IPPs**). The IPPs cover the full 'life-cycle' of information, from the point of collection through to the point of disposal. They include obligations about data security, data accuracy, and rights of access and amendment.

Health information includes information about a person's disability, and health/disability services provided to them. There are 15 health privacy principles (**HPPs**) in the HRIP Act that the

Department must comply with. Like the IPPs, the HPPs cover the entire information 'life-cycle', but include additional principles on anonymity, the use of unique identifiers, and the sharing of electronic health records.

Exemptions to the privacy principles can be found in the two Acts themselves, and in Regulations, Privacy Codes and Public Interest Directions. The disclosure of personal information kept in public registers is covered by separate rules in Part 6 of the PPIP Act.

4.2 Liability and offences

Both the PPIP Act and the HRIP Act contain criminal offences applicable to the Department's staff who use or disclose personal information or health information without authority. For example, there are criminal offences relating to:

- the corrupt disclosure and use of personal and health information by public sector officials (maximum penalty—100 penalty units or imprisonment for 2 years, or both), and
- offering to supply personal or health information that has been disclosed unlawfully (maximum penalty—100 penalty units or imprisonment for 2 years, or both).

Other offences, including relating to dealings with the Privacy Commissioner, are set out in Part 8 of the PPIP Act and HRIP Act.

The Department has policies and privacy controls to minimise the risk of staff committing an offence. For example:

- the Department's Code of Conduct has specific provisions on privacy obligations, including in relation to the authorised access to and use, disclosure and storage of, personal information. The Code also has provisions on the handling of information, including in relation to the confidentiality, misuse, and security of information, and on records management, and
- the Department's Electronic Document and Records Management (**EDRM**) Policy has provisions on information access and security, including that access to information and records held by 'sensitive areas' should be limited and that staff must use information on a 'need to see basis'.

The Department also provides compulsory privacy training to staff to ensure they are aware of their responsibilities in handling personal information appropriately.

5. The Department's responsibilities

5.1 Responsibilities of all Department staff

The Department and all of its staff are required to comply with the PPIP and HRIP Acts. In addition, Ministerial offices and their staff are also required to comply with the PPIP and HRIP Acts. This Plan, together with training and other case-specific advice provided to staff in the course of their duties, is intended to assist staff to understand and comply with their obligations under those Acts.

The Department's Code of Conduct requires staff to be aware of and comply with the PPIP Act and HRIP Act. They must also comply with this Plan. It is every staff member's responsibility to:

- ensure that consent and notification statements are included on each form that collects personal or health information,
- hold personal information securely to avoid loss,

- prevent unauthorised access, use, modification or disclosure, and
- not use or disclose personal information for a purpose other than for which it was collected (unless consent is obtained or another exception applies).

If a staff member is uncertain about whether certain conduct may breach their privacy obligations, they must seek legal advice.

5.2 Responsibilities of the Director, Information and Privacy

The Department's Legal Branch provides privacy advice to individuals and teams within the Department. Members of the public and non-agency staff may also contact the Legal Branch with privacy-related questions. Queries should be directed to:

Director, Information and Privacy
(02) 9228 5871

The Director is responsible for advising Departmental staff (as well as Ministerial staff) about their obligations under the PPIP and HRIP Acts, by:

- ensuring this Plan remains up to date,
- making a copy of this Plan available to all current and incoming staff through the Department's intranet,
- informing staff of any changes to the Plan,
- ensuring relevant privacy documents are consolidated and made available through the Department's intranet,
- making available appropriate privacy training for new and ongoing staff members,
- conducting or arranging staff training sessions on privacy matters as required, and
- being available to provide advice in relation to any questions staff may have about their privacy obligations.

The Director will also ensure the Plan is made available to the public through the Department's website, as part of the Department's obligations to make its 'open access information' publicly available.

In accordance with clause 6 of the Annual Reports (Departments) Regulation 2015 (NSW), the Department's Annual Report will include:

- a statement of the action taken by the Department in complying with the requirements of the PPIP Act, and
- statistical details of any review conducted by or on behalf of the Department under Part 5 of the PPIP Act.

Any amendments to the Plan may be approved by the Director, Information and Privacy according to the current instrument of authorisation under the PPIP Act. A copy of the amended Plan should be circulated to all Departmental staff and the NSW Privacy Commissioner as soon as possible after each amendment, highlighting changes from the previous version.

6. Personal and health information held by the Department

The three most significant examples of personal information held by the Department are set out below.

Note that the Department does not have a health records linkage system (as referred to in HPP 15).

6.1 Employee records for Departmental and Ministerial staff

This includes:

- payroll, attendance and leave records,
- performance management and evaluation records,
- training records,
- workers compensation records,
- occupational health and safety records, and
- records of gender, ethnicity and disability of employees (for equal employment opportunity reporting purposes only).

In 2021, the Department's Secretary gave a direction to employees to be vaccinated (and provide proof of vaccination) against COVID-19. The direction was made in accordance with DPC Circular *C2021-16 Guidance for Government Sector Agencies regarding COVID-19 Vaccinations for their Employees*. The Department's COVID-19 Vaccination Policy (November 2021) provides detail on the health information collected by the Department and notes that it will handle and store such information in accordance with this Plan, the PPIP Act and HRIP Act. A link to the policy is included in section 14 below.

GovConnect provides services to the Department in areas such as payroll, employee services, ICT networks and finance, including accounts payable and general accounting, which means it has access to detailed personal information about the Department's staff. Under the relevant contracts, GovConnect vendors and their personnel must meet strict privacy obligations, including:

- only using data from the Department (including personal information) for the purpose of performing its obligations under the contract,
- ensuring that all data and personal information is stored securely and protected against misuse, loss and unauthorised access, modification and disclosure,
- complying with all relevant privacy legislation and policies as if it were the Department, and
- notifying the Department of any breach of its privacy obligations.

Section 4(4)(b) of the PPIP Act states that personal information is taken to be held by a public sector agency for the purposes of the Act where the information is in the possession or control of a person engaged by the agency in the course of that engagement. Accordingly, where GovConnect has custody of personal information under the contract with the Department, the IPPs may still apply to the Department as if the Department still has custody of that personal information.

6.2 Contact details

This includes:

- government agency CEOs, members of inter-departmental working groups, members of government boards and advisory committees,
- stakeholders and local residents participating in community consultations or Community Cabinets, and the organisations they represent,
- Australia Day Ambassadors,

- people who have applied for community grants,
- people nominated for awards such as Australian of the Year and the Public Service Medal,
- people invited to functions hosted by the Governor,
- office bearers and board members of organisations for whom the Governor is a Patron,
- performers hired for public events,
- volunteers who assist at public events, as well as (where relevant) their dietary requirements, any mobility restrictions, shirt size or drivers licence information, and
- people who enter competitions.

Each of these sets of contact details are held within discrete areas of the Department and are generally not shared within or outside of the Department. For example, the Office of the Governor does not, as a matter of practice, share its contact database with that of the Department's Transformation Group.

The Director, Information and Privacy is responsible for providing advice on any proposal to share sets of contact details held by the Department.

6.3 Correspondence records

This includes:

- contact details of people who have written to or emailed the Premier (including using the Department's online 'Contact the Premier' page),
- details of the nature of their correspondence, which can include sensitive personal information about matters such as ethnicity, religion or sexuality,
- copies of replies to correspondence, and
- records of who, if anyone, their correspondence was referred to.

Correspondents are routinely advised if their letter or email has been referred to a portfolio Minister.

7. Introducing the privacy principles

7.1 Introduction

The privacy principles (IPPs and HPPs) are the standards which the Department adheres to when dealing with personal information and health information.

These principles do not cover the full complexity of privacy law that may arise in all situations but are general propositions that will assist staff in complying with their obligations.

Before relying on any exemption, staff should seek legal advice or contact the Director, Information and Privacy.

7.2 Definitions

Collection of personal information means the way the Department acquires the information. Collection can be by any means. Examples include: a written form, a verbal conversation, an online form, or taking a picture with a camera.

Disclosure means when the Department provides personal information to an individual or body outside the Department. Disclosure includes sharing personal information with other public service agencies.

Health information means personal information that is *also* information or an opinion about:

- a person's physical or mental health or disability,
- a health service provided, or to be provided, to a person,
- a person's express wishes about the future provision of health services to him or her,
- other personal information collected to provide a health service, or in providing a health service, or in connection with the donation of human tissue, or
- genetic information that is or could be predictive of the health of a person or their relatives or descendants.

Holding personal information means the information that is in the Department's possession or control, or is held by a contractor or service provider on our behalf. Most of the privacy principles apply when the Department is 'holding' personal information, which means it remains responsible for what contractors or service providers do on its behalf. This means that information about the Department's staff that is in the physical possession of GovConnect may still be considered to be 'held' by the Department, and therefore the Department remains responsible for how that personal information is handled.

Personal information means 'information or an opinion … about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'. It should be noted that:

- In every case, it is necessary to consider whether each item of information, individually or in combination with other items, is 'about an individual'. This means the Department will evaluate the facts of individual cases before deciding if information is 'personal information', in the same way that the Department is required to determine whether the identity of the individual can reasonably be ascertained.
- For example, personal information can include information that is recorded (e.g. on paper or in a database), but also information that is not recorded (e.g. verbal conversations). It can even include physical things like a person's fingerprints, tissue samples or DNA. The important thing is that it is 'about an individual' and his or her identity can reasonably be ascertained from it.
- Some things are exempt from the definition of 'personal information', including information about a person who has been dead for more than 30 years, and information about an individual that is contained in a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition.
- Also note that 'health information' is sometimes treated a little differently to other types of 'personal information' and has its own definition – see above.

Privacy obligations mean the privacy principles and any exemptions to those principles that apply to the Department.

Sensitive personal information means personal information that is also about a person's race, ethnicity, religion, sexuality, political or philosophical beliefs or membership of a trade union.

Unsolicited information: The PPIP Act provides that personal information is not 'collected' by a public sector agency if the receipt of the information by the agency is unsolicited. Information is not likely to be 'unsolicited' where the Department makes its submission available, e.g. through a complaint filing process.

Use means when the Department uses personal information for some purpose.

We means the Department, including its staff, agents and contractors.

Principle 1: Limiting the collection of personal information

We will only collect personal information if:

- it is for a lawful purpose that is directly related to one of our functions, and
- it is reasonably necessary to have the information.

Key messages and examples

We won't ask for personal information unless we need it. We will especially avoid collecting sensitive personal information if we don't need it. By limiting our collection of personal information to only what we need, it is much easier to comply with our other obligations.

Example: When designing a form, ask yourself: 'do we really need each bit of this information?' If we need to know a person's age to provide age-appropriate services, can we ask for their age or year of birth, not their exact date of birth?

Common exemptions

- Unsolicited information
- Information collected before 1 July 2000.

Principle 2: Anonymity

We will allow people to receive services from us anonymously where lawful and practicable.

Key messages and examples

Example: People making informal enquiries are provided with information about the Department's activities without having to identify themselves.

Principle 3: Unique identifiers

We will only identify people by using unique identifiers if it is reasonably necessary for our functions.

Key messages and examples

Identifiers can assist with efficient record management, but they also pose privacy risks if they are used to match or compile large quantities of data about a person from different sources. For that reason, sharing unique personal identifiers between different organisations is generally prohibited.

A unique personal identifier is not just a person's name or file number. It can be a key (such as a number) which aims to uniquely identify a person – for example so that you can separate all the different people with the name 'John Smith'. A tax file number or a driver's licence number is a unique personal identifier.

The Department avoids collecting unique personal identifiers, although the Department does collect tax file numbers of staff.

Principle 4: How personal information is collected – the source

We collect personal information directly from the person, unless they have consented to collection from a different source or it would be unreasonable or impractical to do so.

We may also acquire personal information from other agencies. Agencies are permitted to disclose personal information to us for the purposes of informing the Premier about any matter.

Key messages and examples

If we need information about Sue, we should ask Sue herself, rather than Jim.

By collecting information direct from the source it is easier for us to comply with other obligations like ensuring the accuracy of information and getting permission for disclosures.

Example: A person attending an event has fainted and a staff member has called the first aid officer. It is OK to ask the person's friend for some health information about them ('do you know if they are diabetic?') because it is unreasonable and impractical to ask the person directly.

Common exemptions

- Unsolicited information
- Where the person is under 16, we can instead collect the information from their parent or guardian (but we don't have to)
- If another law authorises or requires us to collect the information indirectly (i.e. from a different source)
- Information collected before 1 July 2000
- If compliance would, in the circumstances, prejudice the interests of the individual to whom the information relates.

Other relevant points

Where a person lacks some capacity, we can ask their authorised representative for the information instead. But we must also still try to communicate with them directly. The NSW Information and Privacy Commission's Guide on *Privacy and persons with reduced decision-making capacity* explains how to collect personal information from or about a person who has limited or no decision-making capacity.

The NSW Information and Privacy Commission's *Statutory guidelines on the collection of health information from a third party* provides some other examples of when it might be 'unreasonable or impractical' to collect health information directly from the person.

Principle 5: How personal information is collected – the method and content

We will not collect personal information by unlawful means. We will not collect personal information that is intrusive or excessive. We will ensure that the personal information we collect is relevant, accurate, up-to-date, complete, and not misleading.

Key messages and examples

We won't ask for information that is not relevant or that is very sensitive. We must take 'reasonable steps' to ensure we meet this standard, which means considering:

- the sensitivity of the information,
- the possible uses of the information, and
- the practicality and cost of aiming for 'best-practice'.

Example: The Department wants to do a client satisfaction survey of people who attended community consultations on a major new policy document. It is not relevant for the Department to know each participant's home address, date of birth or marital status.

Common exemptions

- Unsolicited information
- Information collected before 1 July 2000.

Principle 6: Notification

When collecting personal information, we will take reasonable steps to tell the person:

- who will hold and/or have access to their personal information,
- what it will be used for,
- what other organisations (if any) routinely receive this type of personal information from us,
- whether the collection is required by law,
- what the consequences will be for the person if they do not provide the information to us, and
- how the person can access their personal information held by us.

Key messages and examples

Individuals providing personal information to the Department have a right to know the full extent of how the information will be used and disclosed, and to choose whether or not they wish to go ahead with providing information. Individuals are typically informed through a 'privacy notice' – which may be available online (on the Department's website or social media pages) or in hardcopy depending on how the personal information is being collected.

An **example** is the privacy notice given to new staff at the time they apply for security access to the 52MP building that explains how the personal information collected through the CCTV and access card systems may be used or disclosed.

Privacy notices should be given in writing but can be given verbally. We need to take 'reasonable steps' to ensure each relevant person receives the notice, which requires considering:

- the sensitivity of the information,
- the possible uses of the information, and
- the practicality and cost of aiming for 'best-practice'.

Where the person lacks some capacity (e.g. because of a brain injury), we must notify their authorised representative, but also still try to communicate with the person directly.

A template privacy notice is available at **Appendix A**.

Common exemptions

- Unsolicited information
- Information collected before 1 July 2000

- If another law authorises or requires us to not notify the person of the collection
- If we're receiving the information as a third-party, the person has already been notified by the organisation that gave us the information.

Other relevant points

When drafting a privacy notice, use the *Template privacy notice* attached in **Appendix A** to this document. Any new projects which might collect personal information should be reviewed by the Department's Legal Branch to ensure an adequate privacy notice is included.

For non-English speaking background clients, the NSW Information and Privacy Commission advises people to contact the translation and interpreting services listed on its website. The website also provides fact sheets in some community languages.

The NSW Information and Privacy Commission's Guide on *Privacy and persons with reduced decision-making capacity* explains how to notify a person who has limited or no decision-making capacity.

Principle 7: Security safeguards

We will take all security measures that are reasonable in the circumstances to protect personal information from loss, unauthorised access, use, modification or disclosure. This includes where the Department engages third-parties to perform services for or on behalf of the Department.

We will ensure personal information is stored securely, not kept longer than necessary, and disposed of securely and appropriately.

Key messages and examples

Security measures could include technical, physical or administrative actions.

To determine what might be 'reasonable steps', we will consider:

- the sensitivity of the information,
- the context in which the information was obtained,
- the purpose for which we collected the information,
- the possible uses of the information, and
- the practicality and cost of the steps proposed to be taken.

Example: We must only provide personal information to a third-party (such as a contractor or service provider) if they need it to do their job. We must take reasonable steps to prevent any unauthorised use or disclosure of the information by the third-party and must bind our contractors to the same privacy obligations as us. The Department uses standard template contracts which contain privacy provisions to manage third-party privacy risk. Where a contract is dealing with particularly sensitive information Legal Branch will advise whether amendments are required to ensure the obligations around privacy are more stringent (for example, including proactive notification provisions for privacy breaches and compliance with the same statute-based privacy obligations as bind the Department).

Example: We must follow the Department's EDRM policy in relation to the retention and destructions of records, noting that the policy states that emails which are corporate records must not be stored in email accounts, so staff should delete them from their email inboxes once saved in Objective.

Other relevant points – data breaches

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to the Department's data. The Department has a Personal Information Data Breach Policy that deals with the process to be followed when a data breach that involves personal information occurs. The Director, Information and Privacy should be immediately notified.

Principle 8: Transparency

We will enable anyone to know:

- whether we are likely to hold their personal information,
- the purposes for which we use personal information, and
- how they can access their own personal information.

Key messages and examples

We have a broad obligation to the community to be open about how we handle personal information. This is different to collection notification, which is much more specific, and given at the time of collecting new personal information.

Example: This Plan will be available on our website. This Plan briefly explains our privacy obligations and sets out the major categories of personal and health information that we hold.

Principle 9: Access

We will allow people to access their personal information and must do so without unreasonable delay or unreasonable expense (see below re the charging of fees). We will only refuse access where authorised by law and will provide written reasons.

Key messages and examples

People should generally be able to see what information we hold about them, with a minimum of fuss.

Our policy is that as much as possible, we will let complainants, clients and staff see their own personal information at no cost, and through an informal request process. Requests may be made verbally or in writing, noting that staff need to verify the identity of the person requesting access before responding, so in some cases may require a request to be in writing. The Director, Information and Privacy can provide advice if a staff member is unsure how to deal with a request.

If there is personal information about other individuals or confidential information about third-parties in any records identified by our searches, then the Director, Information and Privacy will process the request for access, rather than the area that holds the record. This will ensure that the privacy and confidentiality of other people and third-parties can also be properly considered.

We cannot charge people to lodge their request for access. But we can charge reasonable fees for copying or inspection, if we tell people what the fees are up-front. Fees should be no more than we would charge for access under the *Government Information (Public Access) Act 2009*

(NSW) (**GIPA Act**) which is $30 per hour for the work it takes to identify the information sought and consider whether it may be released.

Common exemptions

Another law may prevent us from giving the person access to the information requested.

Other relevant points

If a staff member is unsure about how to respond to a request for access to personal information including whether access can or should be refused or how to provide any information requested in a secure manner then they should refer the request to the Information Access and Privacy Unit to review.

The NSW Information and Privacy Commission's Guide on *Privacy and people with decision-making disabilities* explains how to provide access to personal information held about a person who has limited or no decision-making capacity.

Formal access applications under the GIPA Act will be handled by the Information Access and Privacy Unit in the Department's Legal Branch.

Principle 10: Correction

We will allow people to update or amend their personal information to ensure that it is accurate, relevant, up-to-date, complete and not misleading.

If we are not prepared to amend the personal information because we disagree that it needs changing we will instead allow the individual to attach a statement setting out the amendments sought to the record we hold.

Where possible we will notify any others who had already received the personal information of any changes.

Key messages and examples

Our policy is, as much as possible, to let people update their own personal information at no cost, but we can charge reasonable fees of up to $30 per hour for making an amendment if we tell people what the fees are up-front. However, this does not mean they can just ask us to alter their personnel file without going through the proper processes. Requests should be made in writing to ensure there is no doubt about the correction to be made. Staff should consult the Director, Information and Privacy if they are unsure about how to respond to a request to access and correct personal information.

Example: When a correspondent calls to notify a change in their mailing address we will update their contact details in the Correspondence Management System quickly and for no cost.

Common exemptions

If another law authorises or requires us to not amend the information.

Other relevant points

Any unusual request to amend personal information should be put in writing, and then referred to the Director, Information and Privacy to review.

Principle 11: Accuracy

Before using or disclosing personal information, we will take reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading.

Key messages and examples

We must ensure that personal information is still relevant and accurate before we use or disclose it.

We will take reasonable steps to check the information is accurate. What might be considered 'reasonable steps' will depend upon the circumstances, but some points to consider are:

- the context in which the information was obtained,
- the purpose for which we collected the information,
- the purpose for which we now want to use the information,
- the sensitivity of the information,
- the number of people who will have access to the information,
- the potential effects for the person if the information is inaccurate or irrelevant,
- any opportunities we've already given the person to correct inaccuracies, and
- the effort and cost involved in checking the information.

Example: When People and Culture is investigating a workplace grievance, we will give the person complained about an opportunity to correct the information we are relying on before we make our final decision.

Principle 12: Use

We may use personal information for:

- the primary purpose for which it was collected,
- a directly related secondary purpose within the reasonable expectations of the person, or
- another purpose if the person has consented.

Key messages and examples

We should only use personal information for the purpose for which it was collected or for a directly related secondary purpose that is within the reasonable expectations of the person. We shouldn't go finding new and interesting uses for people's personal information.

Example: If the primary purpose of collecting a complainant's information was to investigate their workplace grievance, directly related secondary purposes within the reasonable expectations of the person for which their personal information could be used by the Department would include independent auditing of workplace grievance files.

Common exemptions

- To deal with a serious and imminent threat to any person
- If another law authorises or requires us to use the information
- Some law enforcement and investigative purposes
- Some research purposes, subject to approval by a Human Research Ethics Committee.

Other relevant points

The primary purpose for which we have collected the information should have been set out in a privacy notice. To use personal information for a purpose set out in the privacy notice is usually OK, but for any other purpose seek legal advice.

If the Department wishes to use the personal information for another purpose, the consent of the relevant individual must be obtained. See the template 'consent wording' in **Appendix A**, or ask the Director, Information and Privacy if you are unsure.

The NSW Information and Privacy Commission has a number of helpful documents:

- *Privacy and persons with reduced decision-making capacity*, which explains how to seek consent for a secondary use of personal information from a person who has limited or no decision-making capacity
- *Statutory Guidelines on Research - Health Records and Information Privacy Act 2002 (NSW)*, which explains how health information can be used for research purposes. It also provides a good rule of thumb for the use of other types of personal information for research purposes
- *Statutory Guidelines on Research – Section 27B*, which explains how agencies may use the exemptions relating to research set out in section 27B of the PPIP Act
- *Checklist: Consent - use or disclosure of personal or health information*, which provides a flowchart to determine whether consent is required before using or disclosing personal or health information.

Principle 13: Disclosure

We will only disclose personal information if:

- at the time we collected their information, the person was given a privacy notice to inform them their personal information would or might be disclosed to the proposed recipient, or
- the disclosure is directly related to the purpose for which the information was collected, and the Department has no reason to believe that the individual concerned would object to the disclosure, or
- the person concerned has consented to the proposed disclosure.

Key messages and examples

We can disclose information in the ways that were notified to the person at the time we collected their personal information. However if we didn't tell the person about the proposed disclosure in a privacy notice, or if it is health information and we want to send it outside NSW, we will usually have to get the person's consent for the disclosure.

Under an exemption in section 27A of the PPIP Act we can also disclose personal information if we are providing the information to another public sector agency. In that situation, our disclosure of the information to the other agency must be 'reasonably necessary' to:

- allow any of the agencies concerned to deal with, or respond to, correspondence from a Minister or member of Parliament, or
- enable enquiries to be referred between the agencies concerned, or
- enable the auditing of the accounts or performance of a public sector agency or group of public sector agencies (or a program administered by an agency or group of agencies).

Determining what is 'reasonably necessary' requires careful judgment. For **example**, if an MP writes to the Premier on behalf of a constituent, and the responsible portfolio Minister responds with additional personal information about the constituent, it may be appropriate to reply direct to the constituent with the additional material – particularly if the additional material is sensitive in nature. The referring MP can be notified that the constituent's enquiry has been responded to directly, without it being 'reasonably necessary' to disclose the constituent's further personal information to their MP. The constituent can then choose whether or not to disclose their own personal information to their MP.

The disclosure and use of personal information between agencies will be allowed where the disclosure is made to an agency within the Premier and Cabinet cluster (i.e. the agencies that are responsible to the Premier) if it is for the purpose of informing the Premier about any matter. The Department does not have any Memorandums of Understanding or other formal referral arrangements in place with agencies in NSW. Note, however, that if a group is transferred from the Department to another agency as a result of machinery of government changes, the Department may enter into a Memorandum of Understanding with the receiving agency for transitional IT services relating to transferred staff and this may involve the transfer or disclosure of personal information.

Tougher rules apply when transferring health information outside of NSW (including to the Commonwealth Government). We can only transfer health information outside NSW if one of the following applies:

- the person concerned has consented,
- it is necessary for a contract with (or in the interests of) the person concerned,
- it will benefit the person concerned and we cannot obtain their consent, but believe the person would be likely to give their consent,
- we reasonably believe it is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the person, another person or to the public,
- we reasonably believe that the recipient of the information is subject to a law or binding scheme equivalent to the HPPs, or
- we have bound the recipient by contract to privacy obligations equivalent to the HPPs.

Common exemptions

- Exchanges of information which are reasonably necessary to allow agencies to deal with or respond to correspondence from Ministers or Members of Parliament
- Exchanges of information which are reasonably necessary for the purpose of referring enquiries between agencies
- To deal with a serious and imminent threat to any person
- To deal with a serious threat to public health or safety (health information only)
- If another law authorises or requires us to disclose the information
- If a subpoena, warrant or 'notice to produce' requires us by law to disclose the information for some law enforcement and investigative purposes
- Some research purposes, subject to approval by a Human Research Ethics Committee.

Other relevant points

The primary purpose for which we have collected the information should have been set out in a privacy notice. To disclose personal information for a purpose set out in the privacy notice is usually OK, but for any other purpose, check with the Director, Information and Privacy first (who can also advise on the use of the template 'consent wording' in **Appendix A** if specific consent from the individual is required).

The Department does not maintain any public registers which contain personal or health information, so the provisions of the PPIP Act regarding the disclosure of personal information contained in such registers are not relevant.

The NSW Information and Privacy Commission has a number of helpful resources when considering disclosure of personal information:

- *Privacy and persons with reduced decision-making capacity*, which explains how to seek consent for a disclosure of personal information from a person who has limited or no decision-making capacity,
- *Statutory Guidelines on Research - Health Records and Information Privacy Act 2002 (NSW)*, which explains how health information can be disclosed for research purposes. It also provides a good rule of thumb for the disclosure of other types of personal information for research purposes,
- *Statutory Guidelines on Research – Section 27B*, which explains how agencies may use the exemptions relating to research set out in section 27B of the PPIP Act, and
- *Checklist: Consent - use or disclosure of personal or health information*, which provides a flowchart to determine whether consent is required before using or disclosing personal or health information.

8. Handling complaints

8.1 Internal Review by the Department

Introduction

Any person may make a privacy complaint, by applying for an 'internal review' of the conduct they believe breaches an IPP and/or an HPP.

Internal review is the process by which the Department manages formal, written privacy complaints about how we have dealt with personal information or health information. All written complaints about privacy are considered to be an application for internal review, even if the applicant doesn't use the words 'internal review'. The Department is required to follow the requirements in Part 5 of the PPIP Act when carrying out an internal review. This Plan is intended to provide guidance on how that can be achieved.

Making a complaint

An application for internal review must:

- be in writing,
- be addressed to the Department,

- specify an address in Australia to which the applicant is to be notified after the completion of the review, and
- be lodged at the Department within six months from the time the applicant first became aware of the conduct that they want reviewed.

The Department encourages the use of the 'Privacy Complaint (Internal Review Application) Form', found at **Appendix B** to this Plan and available on the Department's website. The form provides contact details for where to send it once completed.

An application for internal review can be made on behalf of someone else.

Where the applicant is not literate in either English or their first language and where there is no other organisation making the application on their behalf, staff should help the person to write their application. Staff should use a professional interpreter, if necessary. Applications in other languages will be accepted and translated, and all acknowledgments and correspondence to the applicant will be translated.

Applications for internal review, or any written complaint about privacy, received at any of the Department's offices should be forwarded immediately to the Director, Information and Privacy.

If the complaint is about an alleged breach of the IPPs and/or HPPs, the internal review will be conducted by the Director or by another person (under direction from the Director) who:

- was not involved in the conduct which is the subject of the complaint,
- is an employee or an officer of the Department, and
- is qualified to deal with the subject matter of the complaint.

The Executive Director of the Legal Branch may request the Privacy Commissioner to undertake the internal review on behalf of the Department.

Extensions of time for lodgement

While the PPIP Act allows applicants six months to apply for an internal review from the time the applicant first becomes aware of the conduct, the Department may accept late applications.

Possible acceptable reasons for delay may be:

- the applicant's ill-health or other reasons relating to capacity, or
- the applicant only recently becoming aware of his or her right to seek an internal review, or the applicant reasonably believing that he or she would suffer ill-effects as a result of making an application at an earlier time.

However, late applications that cannot be investigated in a meaningful way because of their age will be declined. In these cases, witnesses may no longer be available, documents may have been destroyed and memories may have faded.

Final decisions on the acceptance of late applications will only be made by the Department's General Counsel, or under his or her delegation. Where the decision is made not to accept an application because it is too old, the reason will be explained in a letter to the applicant.

The internal review process

When the Department receives an internal review application the Director, Information and Privacy will:

- send an acknowledgment letter to the applicant within 5 working days and advise that if the internal review is not completed within 60 days they have a right to seek a review of the conduct by the NSW Civil and Administrative Tribunal, and
- send a letter to the NSW Privacy Commissioner with details of the application. A photocopy of the written complaint will also be provided to the Privacy Commissioner.
    - Under the PPIP Act, the Privacy Commissioner is entitled to make submissions to the Department in relation to the subject matter of the application.

Internal reviews follow the process set out in the NSW Information and Privacy Commission's *Internal Review Checklist*.

When the internal review is completed, the Director, Information and Privacy will notify the applicant in writing of:

- the findings of the review,
- the reasons for the finding, described in terms of the IPPs and/or HPPs,
- any action the Department proposes to take or has taken,
- the reasons for the proposed action(s) (or no action), and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal.

A copy of that letter will be forwarded to the Privacy Commissioner.

Statistical information about the number of internal reviews conducted must be maintained for inclusion in the Department's Annual Report.

8.2 External Review by the NSW Civil and Administrative Tribunal

People may apply to the NSW Civil and Administrative Tribunal (**NCAT**) for an external review of the conduct which was the subject of their earlier internal review application. Information about review in the NCAT can be found in the NSW Information and Privacy Commission's Fact Sheet: *Privacy complaints: Your review rights*. Generally, a person has 28 days from the date of the internal review decision to seek an external review. A person must seek an internal review before they have the right to seek an external review.

The NCAT may decide:

- not to take any action,
- to require the Department to stop any conduct or action which contravenes an IPP or HPP,
- to require the performance of an IPP or HPP,
- to correct information disclosed by the Department, or
- to take steps to remedy loss or damage.

The NCAT may also make an order requiring the Department to pay damages of up to $40,000 if the applicant has suffered financial loss or psychological or physical harm as a result of the conduct.

For more information about seeking an external review, please contact the NCAT:

Website: http://www.ncat.nsw.gov.au/
Phone: 1300 006 228
Post: PO Box K1026, Haymarket NSW 1240
Visit: Level 9, John Maddison Tower, 86-90 Goulburn Street Sydney

8.3 Other ways to resolve privacy concerns

The Department encourages people to try to resolve privacy issues informally before going through the review process, or to at least contact the Director, Information and Privacy to discuss the issue before lodging an internal review.

A person should remember that they have six months from when they became aware of the potential breach to seek an internal review. This six month timeframe continues to apply even if attempts are being made to resolve privacy concerns informally. A person may wish to consider this timeframe in deciding whether to make a formal request for internal review or continue with informal resolution.

Any person can also make a complaint directly to the Privacy Commissioner:

Website: http://www.ipc.nsw.gov.au/
Phone: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Post: GPO Box 7011, Sydney NSW 2001
Visit: Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

9. Data breach and notification

The Department has implemented a Personal Information Data Breach Policy for the purpose of governing how the Department will respond to the unauthorised access to personal information that it holds. The Policy is available to staff on The Hub (see the link provided in section 14 below).

In addition to the processes set out in that Policy, staff must also be aware of and comply with other relevant Commonwealth or international laws:

- Even though the mandatory Commonwealth scheme under the *Privacy Act 1988* (Cth) does not apply to the Department generally, the provisions regarding breaches involving tax file numbers (**TFN**) do. If a TFN data breach occurs that is likely to result in serious harm, then the Department must notify the affected individual and the Australian Privacy Commissioner. See the *Privacy Act 1988* (Cth) and *Privacy (Tax File Number) Rule 2015* (Cth).
- If the Department is provided with data by another government sector agency which is accessed by a data breach the Department may be required to notify the other government sector agency under the *Data Sharing (Government Sector) Act 2015* (NSW).
- The European Union's (**EU**) General Data Protection Regulation (**GDPR**) regime has been given a broad extra-territorial application and could potentially regulate the Department. The Department would be subject to the GDPR requirements if it is offering goods or services to individuals living in the EU or where it monitors the behavior of individuals in the EU (including by tracking web-based activity) where that behavior occurs in the EU.

10. Privacy impact assessment

A Privacy Impact Assessment (**PIA**) may be required to assess any actual or potential effects that an activity, project or proposal may have on personal information held by us. A PIA can also outline ways in which any identified risks can be mitigated and any positive impacts enhanced.

Public consultation and measuring community expectations is an important part of any thorough PIA. A PIA should examine both the positive (privacy-enhancing) and negative (privacy-invasive) impacts, but primarily focus on the negative impacts and how to address such risks.

Privacy risks can be avoided or mitigated by:

- ensuring a project complies with the law,
- ensuring a project meets community expectations,
- making a project less privacy-invasive, and
- making a project more privacy-enhancing.

It may not be possible to eliminate or mitigate every risk, but ultimately a judgement will be made as to whether the public benefit to be derived from the project will outweigh the risk posed to privacy.

To know if a PIA is required, staff should refer to **Appendix C**, which sets out a checklist with some simple yes/no questions. If the answer to one of more of those questions is 'yes', then advice should be sought from the Legal Branch (Director, Information and Privacy) and a PIA should be seriously considered.

There are many benefits in carrying out a PIA, including that this:

- helps to ensure compliance with privacy legislation,
- helps reduce costs later in management time, legal expenses and potential media or public concern by considering privacy issues early,
- assists in anticipating and responding to the public's possible privacy concerns,
- enhances informed decisions-making at the right level, and
- enhances the legitimacy of a project, especially where some compromise or trade-off is necessary.

A PIA will diagnose what risks, benefits, costs and safeguards are involved.

11. Workplace surveillance

In a number of our work locations, cameras, computers or tracking devices may be used to carry out surveillance of our employees in compliance with the *Workplace Surveillance Act 2005*.

A member of the public is not affected by this, other than perhaps being captured by the video recordings, tracking or other surveillance in place.

In general, an employer may carry out a wide range of surveillance, as long as employees are properly notified. This is called 'overt surveillance', or surveillance that everyone is aware of.

Surveillance that employees are not notified about is automatically regarded as 'covert surveillance' and is generally prohibited by legislation, except for the purpose of establishing whether employees are involved in unlawful activity whilst at work. Covert surveillance can only be done with the authority of a Magistrate.

Recording of private conversations is covered by the *Surveillance Devices Act 2007*. Legal advice should be sought for workplace surveillance and the recording of private conversations.

If overt surveillance is in place, employees must be given written notice that includes the following items:

- the kind of surveillance used (e.g. camera, computer, or tracking),

- how the surveillance will be carried out,
- when it will start,
- whether it will be continuous or intermittent, and
- whether the surveillance will be ongoing or for a specified limited period.

Information or the results collected through overt surveillance, cannot be used or disclosed unless the use or disclosure is:

- related to the employment of our employees,
- related to our business activities or functions,
- to a law enforcement agency in relation to an offence,
- related to civil or criminal proceedings, or
- reasonably believed to be necessary to avert an imminent threat of serious violence to persons or substantial damage to property.

A breach of the above restrictions carries a fine. Note that access to the information can be requested by an employee or a person that was captured by the surveillance. Such requests can be made under the PPIP Act or the GIPA Act.

12. Data Analytics Centre and sharing information

The *Data Sharing (Government Sector) Act 2015* (**DSGS Act**) promotes sharing of information for certain purposes which include allowing the government to carry out data analytics. The intent is to identify issues and solutions to better develop government policy, program management, and service planning and delivery.

The DSGS Act provides for the expeditious sharing of information with the Data Analytics Centre (**DAC**). The DAC provides protections in connection with data sharing and ensures compliance with the requirements of the PPIP Act and HRIP Act for privacy protection.

We are required to ensure that health and/or personal information contained in the data that is shared complies with privacy legislation. We are also obliged to ensure that any confidential and commercial-in-confidence information contained in the data to be shared complies with any contractual or equitable obligations of the data provider concerning how it is dealt with.

Before responding to a request from DAC to provide information, we consult internally with the Director, Information and Privacy to obtain relevant advice.

13. Privacy and other legislation relating to personal information

Privacy legislation

- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Privacy Code of Practice (General) 2003* (NSW)
- *Privacy and Personal Information Protection Regulation 2019 (NSW)*
- *Health Records and Information Privacy Act 2002* (NSW)
- *Privacy Act 1988* (Cth)
- *Privacy (Tax File Number) Rule 2015* (Cth)

Other relevant legislation

- *Anti-Discrimination Act 1977* (NSW)
- *Data Sharing (Government Sector) Act 2015* (NSW)
- *Government Information (Information Commissioner) Act 2009* (NSW)
- *Government Information (Public Access) Act 2009* (NSW)
- *Government Sector Employment Act 2013* (NSW)
- *Ombudsman Act 1974* (NSW)
- *Public Interest Disclosures Act 1994* (NSW)
- *Surveillance Devices Act 2007* (NSW)
- *State Records Act 1998* (NSW)
- *Workplace Surveillance Act 2005* (NSW)

Legislation that authorises non-compliance with privacy principles

In the sections of this PMP describing the privacy principles, one of the 'common exemptions' listed against a number of principles is that we are exempt from complying with the principle if another law authorises or requires us to do so. This is because the PPIP Act provides that we are not required to comply with a principle if non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law, including the *State Records Act 1998* (section 25 of the PPIP Act).

The Department receives requests for access to information under the GIPA Act and in response, must consider whether disclosure of the information, which may include personal information, should occur. The GIPA Act provides that there is a public interest consideration against disclosure of information if disclosure of the information could reasonably be expected to contravene an IPP under the PPIP Act or a HPP under the HRIP Act (clause 3(b) of the table at section 14 of the GIPA Act). Under the GIPA Act, the Department is obliged to conduct a balancing exercise to determine if the public interest considerations against disclosure of information outweigh those in favour of disclosure and, if not, the information is disclosed to the applicant (noting that if the information includes personal information about a third person, or concerns that person's business, commercial, professional or financial interests, the Department must first take such steps as are reasonably practicable to consult with that person to determine if they object to release of the information and take their views into account when determining whether to provide access).

14. Department policies affecting processing of personal information

The Department has corporate policies in place to ensure compliance with the PPIP Act and the HRIP Act and promote best practice. These documents are available to staff on The Hub.

Links to the relevant policies current at the time of publishing the PMP are set out below, but please refer to the general Governance – policies page on The Hub to ensure you are accessing the most up-to-date versions of each policy:

- Code of Conduct (February 2022)
  - clauses 5.10 – 5.11 relate to compliance with privacy obligations
  - clauses 5.1 – 5.2 relate to confidentiality
  - clauses 5.3 – 5.6 relate to misuse of information

        - Clauses 5.7 – 5.9 relate to the security of information
    - DPC Mobile Communication Devices Policy (December 2016)
    - Digital Technologies Usage Policy for DPC Staff (December 2016)
    - 52MP Privacy and Surveillance Statement (found on the '52MP DPC Access Card Request' form)
    - DPC Website Privacy Statement
    - Electronic Document and Records Management (EDRM) Policy (September 2016)
    - Personal Information Data Breach Policy (September 2019)
    - DPC COVID-19 Vaccination Policy (November 2021)

APPENDIX A: Template privacy notice and consent

About privacy notices

When collecting personal information, the Department should tell the person:

- whether the collection is required by law;
- what the consequences will be if they do not provide the information;
- what their personal information will be used for;
- who will have access to their personal information;
- who else might receive the information from the Department;
- who will hold/store the information (if not the Department); and
- how they can access or update/correct their information.

The following ***Template privacy notice*** should be used when the Department is collecting personal information in writing, and only intends to use or disclose the information for the purpose for which it is collected.

If any other secondary use or disclosure is contemplated, also use the ***Template consent wording***, below as an additional part of the privacy notice (inserted after the third paragraph of the ***Template privacy notice***).

If personal information is being collected verbally (e.g. over the telephone), see ***Verbal collections*** below.

Template privacy notice

The Department is requesting this information from you so that we can [describe the primary purpose for which this information is being collected – e.g. process your registration for a seminar, assess your job application, investigate your complaint, etc].

We may also [describe any directly related secondary purposes for which the information might be used – e.g. auditing, reporting or program evaluation].

For the same purpose, the Department may provide this information about you to [list any persons or organisations that such information is usually disclosed to, outside of the Department – e.g. the Minister responsible for the subject of their correspondence, or a contractor or consultant].

The Department will not disclose your personal information to anybody else unless we are required to do so by law – for example if the information is needed in an emergency or for a law enforcement purpose.

Providing us with the requested information is not required by law. However, if you choose not to provide us with the requested information, [*describe the main consequences for person if information is not provided – e.g. the Department cannot process your competition entry, or the Department cannot investigate your complaint*].

You may request access to your information at any time. To access or update your personal information, or for more information on our privacy obligations, contact the Department.

The Department will handle and store your personal information in accordance with its Privacy Management Plan and the *Privacy and Personal Information Protection Act 1998* (NSW).

Template consent wording

If the Department wishes to use or disclose personal information for an unrelated secondary purpose (i.e. a purpose not directly related to the primary purpose for which the information was collected), the Department will generally need to seek the person's consent to that secondary use or disclosure.

Consent cannot be a 'requirement' or pre-condition to a transaction. Consent is only valid if it is voluntary, informed, specific, time-limited, and given by a person with the capacity to make decisions about the handling of their personal information.

Ideally, a request for consent will be made at the time the information is collected in the first place. Therefore where a secondary use or disclosure of personal information is anticipated at the time of collection, the following ***Template consent wording*** should be used, as an additional part of the privacy notice, inserted after the third paragraph of the ***Template privacy notice*** (see above).

With your permission, we would also like to [use/disclose] your information to [describe here the intended secondary purpose – e.g. put you on our mailing list for future community events].

□ I consent to my personal information being [*used/disclosed*] for the purpose of [*name the secondary purpose*].

Signature:

Name:

Date:

Verbal collections

When collecting personal information verbally (e.g. during telephone discussions), we can use less formal wording, so long as we explain ***how*** the person's personal information will be used, ***and to whom else*** it will likely be disclosed. If the person asks further questions about whether the information is really needed, then we can go into more depth, and we can also mention their access and amendment rights or offer to let them speak to the Information Access and Privacy Unit.

However, if we need to obtain the person's verbal consent to a secondary use or disclosure, we must explain what it is we are asking, and we must ensure that they understand they are free to say 'no'. We must also make a file-note of what was said.

APPENDIX B: Privacy Complaint (Internal Review Application) Form

1	Name of the agency you are complaining about: **The NSW Department of Premier and Cabinet**
2	Your full name:
3	Your postal address:
4	If you are complaining on behalf of someone else, write their full name here: What is your relationship to this other person? (e.g. parent or lawyer) Is the other person capable of making the complaint him or herself? ☐ Yes ☐ No ☐ I'm not sure
5	What is the specific **conduct** you are complaining about? ('Conduct' can include an action, a decision, or even inaction by the Department. For example the 'conduct' in your case might be a decision to refuse you access to your personal information, or the action of disclosing your personal information to another person, or the inaction of a failure to protect your personal information from being inappropriately accessed by someone else.)
6	Please tick which of the following describes your complaint: *(You can tick more than one)* ☐ collection of my personal/health information ☐ security or storage of my personal/health information ☐ refusal to let me access or find out about my own personal/health information ☐ accuracy of my personal/health information ☐ use of my personal/health information ☐ disclosure of my personal/health information ☐ other ☐ I'm not sure

7	When did the conduct occur? (Please be as specific as you can)
8	When did you first become aware of this conduct?
9	You need to lodge this application within 6 months of the date you have written at Q.8. If more than 6 months has passed, you need to ask the Department for special permission to lodge a late application. If you need to, write here to explain why you have taken more than 6 months to make your complaint:
10	What effect did the conduct have on you?
11	What effect might the conduct have on you in the future?
12	What would you like to see the Department do about the conduct? *(For example:* an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)
13	I understand that this form will be used by the Department to process my request for an Internal Review. I understand that details of my application will be referred to the NSW Privacy Commissioner as required by law, and that the Privacy Commissioner will be kept advised of the progress of the review. I would prefer the Privacy Commissioner to have: ☐ a copy of this application form, or ☐ just the information provided at Q's 5 - 12.

Your signature:

Dated:

SEND THIS FORM, TOGETHER WITH ANY RELEVANT INFORMATION, TO:

Information and Privacy Unit
Legal Branch
NSW Department of Premier and Cabinet
GPO Box 5341
SYDNEY NSW 2001

Or email: infoandprivacy@dpc.nsw.gov.au

You should keep a copy for your own records too.

APPENDIX C: Privacy Impact Assessment Checklist

The following checklists assists in determining whether a privacy impact assessment (**PIA**) is required during the design and implementation of policies and programs.

If the answer to any question is 'yes' then a PIA is highly advisable

Does the policy/project/program require:		Yes	No
1	The collection of personal information by the Department; either compulsorily or voluntary?		
2	A new use of personal information that is already held by the Department?		
3	A system of disclosure of personal information; either to other NSW agencies, other jurisdictions, private entities or individuals?		
4	Restricting the access of individuals to their own personal information?		
5	Confidentiality provisions relating to personal information?		
6	The storage, securing or retention of personal information?		
7	Identity verification such as the requirement to sight documents?		
8	Establishing a new identification system or creation of a new identification marker such as unique numbers for individuals?		
9	Data matching of personal information with any other entities, including other NSW agencies or Commonwealth agencies?		
10	Any transferring or disclosure of personal information to any jurisdiction outside NSW, including to the Commonwealth?		
11	Any research or compilation of statistics that relies on personal information whether or not it is de-identified?		
12	Coercive regulatory powers such as any powers of search, seizure, entry or detention?		
13	Monitoring or surveillance of individuals including their behaviour or communication?		

These matters are not exclusive and not necessarily comprehensive. They are intended only as a guide as to the most obvious examples, although preparation of a PIA may still be warranted in other circumstances. See further detail on PIAs, including contact details for the Legal Branch, in section 10 above.