information and privacy commission
new south wales

Privacy Management Plan

June 2014

Contents

Email: ipcinfo@ipc.nsw.gov.au

Phone: 1800 472 679

Mail: GPO Box 7011 Sydney NSW 2001

Introduction

This plan explains how we (the Information and Privacy Commission) manage personal and health information in line with the NSW privacy laws.

Why we have a privacy management plan

We have a Privacy Management Plan (plan) because we want our stakeholders and staff to know how we manage personal information. With this plan we also acquit our compliance with s33 of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act).

The plan explains how we manage personal information in line with the PPIP Act and health information under the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act).

It also explains who a person can contact with questions about the personal or health information we hold, how they can access and amend their information and what to do if they think we may have breached the PPIP Act or the HRIP Act.

We also use this plan to train our staff about how to deal with personal and health information. This helps to ensure that we comply with the PPIP Act and the HRIP Act.

Please refer to **Appendix A** for more information about the PPIP Act, the HRIP Act and other privacy-related instruments.

What this plan covers

S33(2) of the PPIP Act sets out the requirements of this plan. This plan must include:

- information about how we develop policies and practices in line with the PPIP Act and the HRIP Act
- how we train staff in these policies and practices
- our internal review procedures
- anything else that we consider relevant to the plan in relation to privacy and the personal and health information we hold.

We also referred to our own privacy management plan resources when writing this plan. The "Guide to making privacy management plans" and the "Privacy management plan assessment checklist for agencies" are available on our website.

When we review this plan

We will review this plan every 12 months. We will review the plan earlier if any legislative, administrative or systemic changes affect how we need to manage personal and health information.

About us

Who we are

The Information and Privacy Commission NSW (IPC) is an independent statutory authority that administers New South Wales legislation dealing with privacy and access to government information. The IPC was established on 1 January 2011 to support the Information Commissioner and the Privacy Commissioner in fulfilling their legislative responsibilities and functions.

We administer the following laws:

- *Government Information (Public Access) Act 2009* (GIPA Act)
- Government Information (Public Access) Regulation 2009
- *Government Information (Information Commissioner) Act 2009* (GIIC Act)
- *Privacy and Personal Information Protection Act 1998* (PPIP Act)
- Privacy and Personal Information Protection Regulation 2009
- Privacy Code of Practice (General) 2003
- *Health Records and Information Privacy Act 2002* (HRIP Act)
- Health Records and Information Privacy Regulation 2006
- Health Records and Information Privacy Code of Practice 2005.

These laws govern:

- the right to access government information from NSW public sector agencies
- how NSW public sector agencies manage personal information
- how NSW public sector agencies and the private sector manage health information.

For more detailed information about us and the legal framework applying, please refer to our website.

Our functions

Our core functions are set out in s17 of the GIPA Act, s14 of the GIIC Act, s36 of the PPIP Act, and s58 of the HRIP Act.

Generally, our functions are to:

- **promote** the GIPA Act, PPIP Act and HRIP Act and educate NSW public sector agencies and the public about a person's access and privacy rights
- **assist** our stakeholders to understand and use these laws
- **review** agency decisions, oversee internal reviews, investigate and resolve complaints
- provide **feedback** to Parliament about the laws we administer and about developments in other relevant laws and technology.

The Information Commissioner also has the function to receive "public interest disclosures" under the *Public Interest Disclosures Act 1994* (PID Act).

The Privacy Commissioner has functions under other legislation, including a role to advise the Children's Guardian about the suitability of a person authorised to undertake audit declarations by exempt workers under the *Child Protection (Working with Children) Act 2012* and to approve protocols under the *Roads and Transport Act 2013.*

We also manage the staffing, systems and administration of our office.

Our stakeholders

We may collect personal and health information from our stakeholders in order to do our work, such as:

- members of the public
- NSW public sector agencies (including Ministers' offices, State owned corporations, local councils and universities)
- private sector companies
- solicitors and other legal representatives
- non government organisations.

How we manage personal and health information

We collect and receive many different kinds of personal information in order to conduct our functions.

When we use the term "personal information" we mean it according to the definition in the PPIP Act:

- information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion;
- including such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

In this section, a reference to personal information is also a reference to health information.

Enquiries

We handle enquiries from our stakeholders about the right to government information and privacy protection in NSW.

People can make enquiries:

- over the phone (we do not record telephone conversations, however we do have a voicemail service)
- in writing (email, letter, fax, online form)
- in person (at the counter and at events).

Personal information people give us

People may provide us with personal information when they contact us with enquiries. This can include names, contact details, opinions, health conditions and illnesses, family relationships, housing or tenancy information, work history, education and criminal histories. The amount of personal information varies for each enquiry. In some cases, people may provide us with significant amounts of personal information.

Usually people only give us their own personal information, however sometimes they might give us personal information about other people with or without their knowledge. Sometimes people give us more personal information than we would either ask for or need to deal with their enquiry.

How we collect personal information

We decide what level of personal information is appropriate to be collected for each enquiry on a case-by-case basis, with the understanding that the detail we collect must contain enough information to be an accurate record of the issue and assistance given but should not contain unnecessary personal information.

If someone writes to us we generally keep a full copy of whatever they sent, however if someone calls us over the phone and gives us a lot of background information we may decide not to record all personal information if it is irrelevant to the enquiry. For example, we might make a general note such as “concerned about employer disclosing details of an illness”, without recording details about the illness itself.

The provision of any personal information is entirely voluntary, and we give people the option of remaining anonymous if preferred. When someone stays anonymous we only record the gender of the person who contacted us. We do not ask for or record contact details unless the person sent us a written enquiry or wants us to call them back or send them information.

Our phones display the number of the person who called (except for private/silent numbers), but we do not keep a record of these numbers or use them. We do not electronically record telephone conversations.

Sometimes we may not be able to provide the best assistance without knowing at least some personal information. For example, if the enquiry is complex we might ask someone to send us details of the issue in writing. In these cases it is up to the person who called to decide whether they want to continue the enquiry or not.

Storage, accuracy and use of personal information

We record details of each enquiry on electronic enquiry registers, and store electronic and hard copies of written enquiries. No one other than our staff can access these registers.

We make sure personal information is accurate before using it. For example we check contact details directly with the person to make sure we have recorded them correctly and ask people to spell their names where necessary. We do this to make sure we send personal information to the right person.

We use this personal information only for dealing with enquiries from that particular person. We may look at past enquiries from a particular person to get background information if we receive more enquiries or a complaint or review request from that person. We use issues raised in enquiries to identify enquiry trends.

We do not disclose information about a particular enquiry to anyone outside our office without the consent of the enquirer.

Reviews, complaints and investigations

Our casework team:

- conducts external reviews of agency decisions on access applications for government information
- handles complaints about agency conduct under the GIIC Act
- investigates agency compliance with the GIPA Act
- handles public interest disclosures made to the Information Commissioner
- oversees internal reviews that NSW public sector agencies conduct in response to complaints about how they manage personal and health information under the PPIP Act and HRIP Act
- handles complaints about how NSW public sector agencies manage personal information under the PPIP Act
- deals with complaints about how NSW public sector agencies and private sector health providers manage health information under the HRIP Act
- investigates agency compliance with the PPIP Act and HRIP Act
- provides general advice to our stakeholders on privacy-related issues.

The Commissioners have the right to appear in access-related and privacy-related external reviews conducted by the NSW Civil and Administrative Tribunal (NCAT).

How we collect personal information

We collect personal information in writing, by email, through the website enquiry form, over the phone, by fax and in person at the counter. The IPC also collects personal information through a request for assistance form.

The IPC receives personal information from people when they seek an external review or make a complaint to either the Information Commissioner or the Privacy Commissioner.

The IPC receives notifications of internal reviews from the NSW public sector agencies conducting them. People may send their internal review application to us to pass on to the agency to conduct the internal review. They may also give us personal information when making complaints to the Privacy Commissioner.

People will usually send us their own personal information, however quite often they also give us personal information about other people.

Sometimes people may be able to seek a review or make a complaint anonymously. The IPC oversees privacy internal reviews conducted by NSW public sector agencies including those matters where the internal review applicant remains anonymous. The IPC is usually unable to conduct anonymous external reviews with regard to the GIPA Act. We encourage anyone who is considering exercising their rights under the PPIP Act, HRIP Act, or GIPA Act anonymously to contact us to discuss their options.

We may ask people to send us further personal information relating to the review or complaint. Our file notes may sometimes contain personal information.

In addition, the Information Commissioner has the right under the GIPA Act to access information from NSW public sector agencies when it relates to the Commissioner's functions. The Information Commissioner can also enter the premises of NSW public sector agencies and access their information.

Similarly, the Privacy Commissioner has the right under the PPIP Act and HRIP Act to require a person or agency (and organisation under the HRIP Act) to provide information to the Privacy Commissioner when it relates to the Commissioner's functions.

We also receive and collect personal information when we appear in NCAT proceedings, either at the proceedings or from submissions received from the parties.

We aim to tell applicants how we will manage their personal information when they seek our assistance, however under the laws we administer we do not give people details of personal information we receive about third parties unless legally required to do so.

How we use and disclose personal information

We use the information we collect to:

- conduct or oversee reviews
- refer a complaint to a relevant authority
- advise the Commissioners, our staff and our stakeholders on recurring trends and issues
- educate our stakeholders about particular issues (through published reports).

Sometimes we publish reports that relate to our casework. We seek consent from affected people if any of their personal information is contained in a review report. If people do not consent to their personal information being published we may publish the report with their personal information de-identified.

The IPC discloses the name of review applicants to the agency that made the decision and seeks consent from complainants before disclosing their names to the agency. If a person does not give consent we will assess the complaint to see how we can deal with it. The IPC may discuss personal information with the relevant agency when conducting a review, complaint or investigation.

We include relevant personal information in the reports we write. We generally send these reports to the parties to the case.

When we are involved in NCAT cases, we may disclose personal information relevant to that particular case.

We may also refer issues to other oversight bodies (see section below).

Apart from the above, we do not disclose personal information to anyone not directly involved in a complaint, investigation or review case, unless authorised or required to do so by any law.

We are particularly careful when dealing with sensitive personal information such as racial origin, health information or sexuality.

The GIPA Act restricts the IPC from disclosing any information to the review applicant or complainant where the agency claims there is an overriding public interest against disclosure and has decided not to release the information. This quite often includes personal information.

Under s47 of the PPIP Act, the Privacy Commissioner may:

- refer a complaint relating to privacy for investigation or other action to a relevant authority considered by the Privacy Commissioner to be appropriate in the circumstances;
- communicate to the relevant authority any information that the Privacy Commissioner has obtained in relation to the complaint; and
- only refer a complaint to a relevant authority after appropriate consultation with the complainant and the relevant authority, and after taking their views into consideration.

How we store personal information

We store personal information electronically and in physical files. We have a "clean desk" approach, which means all our physical files are locked up at the end of the day or when not in use.

Sometimes we take our files off-site such as to attend external reviews at the NCAT or attend agency premises. We do not leave sensitive files unattended and do not let anyone else access them. We use encrypted USB devices where possible.

Public interest disclosures

People have the right to make public interest disclosures to the Information Commissioner about potential breaches of the GIPA Act by government agencies.

The Information Commissioner and the Principal Review Officer are generally the only staff members in our office who have access to and deal with public interest disclosures. PID files are locked in secure cupboards and electronic files, and access to the information is restricted on a need-to-know basis.

We do not generally disclose the identity of the complainant to anyone, including the agency against which the public interest disclosure was made. Sometimes, however, it may be difficult to properly investigate the disclosure without disclosing the identity of the complainant. In these cases the Information Commissioner or the Principal Review Officer will speak with the complainant about courses of action.

Referrals to other oversight bodies

Under the GIIC Act, the Information Commissioner can provide information to:

- the NSW Ombudsman
- the Director of Public Prosecutions
- the Independent Commission Against Corruption
- the Police Integrity Commission.

The Information Commissioner also has a Memorandum of Understanding with the NSW Ombudsman outlining how the two agencies will share information between each other. This is available on our website.

The Privacy Commissioner has entered into an information sharing and complaint referral arrangement with:

- the NSW Ombudsman
- the Health Care Complaints Commission
- the Anti-Discrimination Board
- the Legal Services Commissioner.

This document is also available on our website.

The NSW Privacy Commissioner established Collaboration Principles with the Australian Privacy Commissioner.

Section 67(2) of the PPIP Act states that the Privacy Commissioner is not prevented from:

furnishing any information relating to

(a) a matter arising under another State, a Territory or the Commonwealth: or

(b) an undertaking that is or was being carried out jointly by New South Wales and another State, a Territory or the Commonwealth

to a person exercising under a law of that other State, that Territory or the Commonwealth functions similar to those exercised by the Commissioner under this Act or any other Act.

Section 47(3) of the PPIP Act states that:

the Privacy Commissioner may only refer a complaint to a relevant authority after appropriate consultation with the complainant and the relevant authority, and after taking their views into consideration.

Communications and stakeholder engagement

Our communications and stakeholder engagement team help us to promote our Acts and assist our stakeholders to understand and use them.

Subscriber, mailing and contact lists

We keep subscriber, mailing and contact lists that contain personal information from people who have asked to be included in our mailing and contact lists. We do not generally collect details apart from names, email addresses and agency type.

Our main lists that collect personal information are:

- our newsletter subscriber list – to email our newsletter to those who have requested subscription
- community stakeholders list – to contact non government organisations and other members of the community about access and privacy
- the practitioners list – to communicate with right to information and privacy practitioners within our jurisdiction.

We do not collect personal information without consent, and we advise people how we will manage their personal information when they provide it to us. We keep our lists separate from each other and use them only for the purpose for which we advised we would use them. We do not disclose individual email addresses when sending out bulk emails.

Our communications staff are the only people in our office who access these lists, however we have an agreement with a third party to store and manage our lists for us and we are satisfied that they manage our information appropriately.

We rely on people providing their accurate personal information to us and we are careful to enter the correct information. Anyone can subscribe or unsubscribe themselves from our newsletter list, or contact us to change their details on other lists. We do not destroy these lists; we keep the lists as long as they remain current. We can delete individual entries on request or if we receive error messages in response to our communications.

Training sessions

We deliver training sessions to our stakeholders. We collect registration details of the people who formally sign up to our public events. These details usually include names, email addresses, contact numbers and agency name (if applicable). We only use this information to confirm numbers and communicate with participants about that particular event.

When providing training in-house for an agency, we fill out an attendance list and provide it to the agency for their records. These lists contain name and position only.

We only collect health information if a participant has any special requirements or adjustments needed for the training. This information is not retained after the event.

We store this information electronically on our share drive, in paper form and with a third party provider.

We ask for feedback from our participants and give them the option of remaining anonymous. We do not ask for names or contact details. We use this feedback to improve our training sessions and material. We may publish collated feedback and comments but do not identify people.

If someone has an enquiry that we cannot answer straight away we offer to take down their details so someone in our office can get back to them.

Community outreach

We participate in community events and visit different communities. We may hold these events or participate in events held by other agencies or organisations.

We may collect very basic information such as number of visitors to our stall and may collect demographic information such as gender, the kinds of questions asked and what resources we provided. We do not identify individuals. We do not collect personal information such as names and contact details unless someone asks for further assistance from us.

We do not give personal information to other agencies or organisations that may have participated in the event.

Depending on the event, we may intentionally or unintentionally collect health information or sensitive personal information about someone. For example, if we participate in a session designed for people with disabilities or people from a particular cultural or racial background it could be deduced that someone has or is likely to have a disability or has a particular cultural or racial background.

Sometimes we seek voluntary completion of surveys to help us identify current issues, and may also collect different kinds of demographic data. We ensure any proposed survey or other kind of collection complies with the PPIP Act and HRIP Act.

Conferences and other events

We sometimes deliver or participate in other events including conferences, seminars etc. We will consider the PPIP Act and the HRIP Act when we are organising events and aim to notify affected people how we will manage their personal and health information if we collect it, such as on registration forms.

If we use an event management company to assist with delivering an event, we will make sure it has appropriate privacy management practices in place. For more information please refer to our section on private sector companies and contractors.

Website publishing, photography, filming and media

We currently maintain one website: www.ipc.nsw.gov.au.

We use our website to promote our Acts and publish resources to help our stakeholders understand and use our Acts. We would not publish personal or health information on our website without permission.

We also collect enquiries and feedback through an online form on our website. For more information about how we deal with this information, please refer to our section on enquiries.

Our website data is stored on secure servers and on our share drive.

We may take photos or film events that we hold or participate in and use them for promotional purposes. We will always seek permission of people (including our own staff) before we take photos or film events and advise how we will manage that information. We ask people to sign a consent form. We will respect the wishes of those who do not wish to be photographed or filmed.

We store photos and footage electronically on our share drive.

Our communications and stakeholder engagement team deal with media enquiries. We do not provide personal or health information to the media in response to their enquiries without consent.

Policy development

Feedback and consultation papers

People can give us feedback on the laws we administer. While we do not ask for it, they may decide to give us personal information such as contact details, personal opinions, stories, experiences and backgrounds. They may also give us personal information of other people. We may ask for further personal information but only to clarify the issue being raised.

We also publish consultation papers to seek feedback on particular aspects of our laws. We do not ask for more information than what is helpful to us. We may promote our consultation through various agency, non-government organisation and media channels, however participation is voluntary.

We store this information on our share drive or in hard copy files, and generally do not disclose personal information.

We rely on people to give us accurate information and to contact us to amend it if necessary.

We use personal information to help us understand the context of the issues being raised and decide whether to write reports or bring issues to the attention of NSW Parliament, the Attorney General or other relevant individuals, Ministers or public or private sector organisations.

When we write reports and make findings or submissions publicly available we do not identify people unless we have already sought the consent of the relevant people or notified them in advance of how we would disclose the information they give to us.

Privacy-related policies

We consult when we develop new policies or procedures or amend them in way that would change how we manage personal and health information. We do this to make sure we comply with the PPIP Act and HRIP Act.

While an independent Commission, we comply with relevant policies written by the Department of Justice (DJ), particularly human resource and information technology related policies. Please refer to **Appendix B** for a list of key privacy-related policies.

Staff, contractors and visitors

Recruitment

When people apply for jobs at our office they send us personal information such as their names, contact details and work history. Our business support team gives this information to the convenor of the panel for that particular position (stated on the job advertisement) in electronic or physical files.

The convenor of the panel does not disclose this personal information to anyone in the IPC except for business support and the relevant Commissioner(s). Convenors store this information securely. The convenor does not disclose the information to anyone outside the IPC except for the human resources unit at DJ and other panel members.

After recruitment is finalised, convenors give all personal information back to the business support team to send to the human resources at DJ. They retain information relating to successful applicants and eligibility lists for three years. Unsuccessful applications are destroyed.

Successful applicants are invited to fill out various forms to commence employment with the IPC with further personal information such as bank account details, tax file number, emergency contacts and any disabilities that may impact their work.

These forms also encourage people to provide sensitive personal information such as racial and cultural information for statistics about the wider NSW public sector. These items are voluntary.

These forms are sent to the DJ human resources unit to be used for employment purposes such as payroll and setting up personnel files. The business support team keep copies of this information in secure storage areas.

Staff

At times we collect and manage personal information about our staff, such as:

- medical conditions and illnesses
- next of kin
- education
- family and care arrangements
- secondary employment
- conflicts of interest.

We collect this information for various reasons such as leave management, workplace health and safety, and to operate with integrity.

We do not to ask for more personal information than what is actually required. We advise staff when collection is voluntary or mandatory, and of any possible consequences of not providing it to us.

We collect this information directly from our staff and aim to notify them how we will manage their information.

Usually our staff will disclose this information to their direct manager or the business support team. This information may also be provided upward through relevant reporting lines to the relevant Commissioner(s) depending on the situation. The information will also be forwarded to the human resources unit at DJ.

We do not disclose this information to anyone else without consent.

Private sector companies, government agencies and contractors

We may use private sector companies, contractors, or even other government agencies to provide services to or for our office. If they will have or are likely to have access to personal information we make sure that they manage personal and health information in line with the PPIP Act, HRIP Act and information security policies. We might do this by:

- asking for evidence of their information-handling processes
- inserting a privacy clause into our contracts.

We will also consider how a private sector company or contractor will manage personal or health information we give them before engaging with external service providers. We give priority to addressing the issues we identify.

Here is a list of external entities that may manage or collect personal information on our behalf.

- We have a service level agreement with the Department of Justice to provide our human resources and information technology systems and support
- We use a secure shredding company for the destruction of sensitive documents
- We use a marketing company manages our mailing lists and newsletter
- NSW Roads and Maritime Services hosts the GIPA reporting tool for agencies
- We procure temporary staff from providers under government contract when necessary
- We may use event management companies to host events and manage registrations
- We may use other independent contractors for various purposes.

Visitors

We use a visitors' book to record the names of people who enter our office beyond the public area. This book is displayed on our front counter. We collect this information for workplace health and safety purposes.

Systems and administration

Systems and information management

We have a service agreement with the Department of Justice (DJ) to provide our information technology and HR systems and support.

All our electronic information is stored on secure information systems from our shared service provider. The systems comply with the international standard of information security ISO/IEC 27001 as per DJ's Information Security Management System (ISMS) Policy. Our servers are backed up daily. Our networks are secure and require individual logins. Our staff do not give out passwords to anyone or let anyone else use their computer login.

Our information is classified in line with the NSW State Records Keyword AAA Thesaurus.

We aim to comply with State Records legislation. We are working on retention and disposal rules for our general administration and functional information.

We consult with our privacy team when considering and implementing new information management systems and software. We do this to make sure that any new system will comply with the PPIP Act and HRIP Act. If we are not satisfied with how a system or software will manage personal or health information we give priority to addressing the issues we identify.

Physical security

Our hard copy information is mainly located in our office at Level 17, 201 Elizabeth Street, Sydney NSW 2000. We archive older physical files in a secure storage facility in compliance with the *State Records Act 1998*. Our staff have keycard access to our office. Visitors cannot enter without our permission, and we do not leave visitors unsupervised. Our office is locked outside of business hours.

We keep physical files securely stored when we are not using them. We do not leave sensitive information on the printer and use secure printing where appropriate.

Our staff have unique user accounts and passwords to access our computer systems. Our staff do not give out passwords to anyone or let anyone else use their computer login in accordance with our information security policy.

We use locked bins for sensitive documents that need to be destroyed.

Electronic and physical mail handling

We address outgoing mail and email appropriately, and refer incoming correspondence to the correct team or person.

We comply with electronic mail policies.

We record details of all incoming and outgoing mail on a mail register.

How to access and amend personal and health information

People have the right to access personal information we hold about them.

They also have the right to amend their own personal or health information we hold, for example if they need to update their contact details.

We must provide access to or amend personal or health information without excessive delay or expense. We do not charge any fees to access or amend personal or health information.

Informal request

We encourage people wanting to access or amend their own personal or health information to contact us to request it.

We encourage people to contact the staff member or team managing their information.

- Enquiries: contact our main enquiry line.
- Case-related: contact the team or staff member handling the matter.
- Newsletter subscriptions: add or remove own details through our website.
- Staff information: speak with our business support team or contact the HR department at DJ.

A person does not need to put an informal request in writing. If necessary, we will ask them to verify their identity or make a formal application instead.

We aim to respond to informal requests within **5 working days**. We will tell the person how long the request is likely to take, particularly if it may take longer than first expected.

We will contact the person to advise the outcome of the request. In some cases, particularly if it is sensitive information, we may ask them to make a formal application.

If a person is unhappy with the outcome of an informal request, they can make a formal application to us.

Formal application

People also have the right to make a formal application to access or amend personal or health information. A person does not need to ask informally before making a formal application, and a person can make a formal application if they have already asked informally.

A person can make a formal application to the Privacy Contact Officer by email, fax or post (contact details on page 17). The application should:

- include the person's name and contact details (postal address, telephone number and email address if applicable)
- state whether the person is making the application under the PPIP Act (personal information) or HRIP Act (health information)
- explain what personal or health information the person wants to access or amend
- explain how the person wants to access or amend it.

We aim to respond in writing to formal applications within **20 working days**. We will contact the person to advise how long the request is likely to take, particularly if it may take longer than expected.

If a person thinks we are taking an unreasonable amount of time to respond to an application, they have the right to seek an internal review. Before seeking an internal review, we encourage people to contact our office to ask for an update or timeframe.

Why we might not give access to or amend personal or health information

If we decide not to give access to or amend personal or health information, we will clearly explain our reasons. For example, when we undertake an external review under the GIPA Act we are generally restricted from giving people access to information we have obtained from NSW public sector agencies for the purposes of conducting or overseeing the review.

We may however release the information if the agency or person explicitly consents to its release.

If a person disagrees with the outcome of an application, they have the right to seek an internal review.

Limits on accessing or amending other people's information

We are usually restricted from giving people access to someone else's personal and health information. The PPIP Act and the HRIP Act give people the right to access their own information; they generally do not give people the right to access someone else's information.

Under s26 of the PPIP Act, a person can give us consent to disclose their personal information to someone that would not normally have access to it.

Under s7 and s8 of the HRIP Act, an "authorised person" can act on behalf of someone else. The HPPs also contain information about other reasons we may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety of the individual, to find a missing person or for compassionate reasons.

If none of the above scenarios are relevant, a third party could also consider making an application for access to government information under the GIPA Act.

Review rights and complaints

Internal review by our office

People have the right to seek an internal review under the PPIP Act if they think that we have breached the PPIP Act or HRIP Act relating to their own personal or health information. People cannot seek an internal review for a breach of someone else's privacy, unless they are authorised representatives of the other person.

People must apply for an internal review within **six months** from when they first became aware of the breach. We may also consider a late application for internal review.

Internal review process

A person can seek an internal review by filling out the internal review form available on our website and sending it to our Privacy Contact Officer by email, fax, post or at our counter (details on page 22) along with any relevant information.

The Privacy Contact Officer will conduct the internal review unless the internal review is about the conduct of the Privacy Contact Officer. In this case the Information Commissioner will appoint someone else within our office to conduct the internal review.

We aim to:

- acknowledge receipt of an internal review within **5 working days**
- complete an internal review within **60 calendar days**.

The Privacy Contact Officer will inform the person of the progress of the internal review, particularly if it is likely to take longer than first expected.

The Privacy Contact Officer will respond to the person in writing within **14 calendar days** of deciding the internal review. This is a requirement under the PPIP Act.

If a person disagrees with the outcome of an internal review or is not notified of an outcome within 60 days, they have the right to seek an external review.

The Privacy Commissioner's role in internal reviews

Usually when an agency receives an internal review it must notify the Privacy Commissioner of the internal review and of the proposed outcome. The Privacy Commissioner is entitled to make submissions to the agency of her view of the matter.

While the Office of the Privacy Commissioner forms part of the IPC and is not a separate, independent entity in the same way as it is to other agencies, we still follow the same notification process. The Privacy Commissioner is committed to making submissions on the internal review in an objective manner.

External review by the NSW Civil and Administrative Tribunal (NCAT)

A person can seek an external review if they are unhappy with the outcome of an internal review we have conducted or do not receive an outcome within 60 days.

To seek an external review, a person must apply to the NSW Civil and Administrative Tribunal (NCAT). 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.

NCAT has the power to make binding decisions on an external review.

For more information about seeking an external review including current forms and fees, please contact the NCAT:

Website: http://www.ncat.nsw.gov.au/ncat/index.html

Phone: (02) 9377 5711

Visit/post: Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

The NCAT cannot give legal advice, however the NCAT website has general information about the process it follows and legal representation.

Other ways to resolve privacy concerns

We encourage people to try to resolve privacy issues with us informally before going through the review process, or at least contact the Privacy Contact Officer before lodging an internal review to discuss the issue.

A person can raise their concerns with us by:

- contacting the Privacy Contact Officer
- making a complaint directly to the Privacy Commissioner
- using our complaint process (available on our website).

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 time frame continues to apply even if attempts are being made to resolve privacy concerns informally. A person may wish to consider this time frame in deciding whether to make a formal request for internal review or continue with informal resolution.

Complaint to the Joint Parliamentary Committee

If a person wishes to complain about either of the Commissioners, they can write to the Joint Parliamentary Committee that oversees our office. While the Joint Committee cannot reconsider or investigate a matter, they can review how the Commissioners have exercised their functions. See our complaint process for further information.

Promoting the plan

Executive and governance

Our executive team is committed to transparency about how we comply with the PPIP Act and HRIP Act.

Our executive team reinforces transparency and compliance with the PPIP Act and HRIP Act by:

- endorsing the plan and making it publicly available
- providing a copy of the plan to relevant oversight bodies such as the Risk and Audit committee and the Parliamentary Joint Committee on the Office of the Ombudsman and the Police Integrity Commission
- making privacy a standard agenda item in their executive meetings
- reporting on privacy issues in our annual report in line with the *Annual Reports (Departments) Act 1985* (NSW)
- confirming support for privacy compliance in the strategic plan and code of conduct
- identifying privacy issues when implementing new systems
- using it as part of induction for new staff, contractors etc.

Our staff

We make sure that our staff are aware of and understand this plan, particularly how it applies to the work they do. Privacy breaches are more likely to occur when a plan is not sufficiently relevant to the work that is actually done in an agency. With this in mind, we have written this plan in a practical way so our staff can understand what their privacy obligations are, how to manage personal and health information in their work and what to do if unsure.

We make our staff aware of their privacy obligations by:

- publishing the plan in a prominent place on our website
- including the plan in induction packs and offering training quarterly or as required
- providing refresher, specialised and on-the-job privacy training
- highlighting the plan at least once a year (e.g. during Privacy Awareness Week).

When our staff have questions about how to manage personal and health information and this plan does not directly answer them, they should consult their manager or our Privacy Contact Officer.

Public awareness

This plan is a guarantee of service to our stakeholders of how we manage personal and health information. Because it is central to how we do business, we will make this plan easy to access and easy to understand for people from all kinds of backgrounds. Additionally, we are required to make this plan publicly available as open access information under the GIPA Act.

We promote public awareness of this plan by:

- writing the plan in plain English
- publishing the plan in a prominent place on our website
- providing hard copies of the plan free of charge on request
- translating the plan into other languages on request or in other formats as required
- referring to the plan in our privacy notices
- telling people about the plan when we answer questions about how we manage personal and health information.

Contacting us

Privacy Contact Officer

Our Executive Director has been given the delegation of Privacy Contact Officer.

The Privacy Contact Officer:

- responds to enquiries about how we manage personal and health information
- responds to requests for access to and amendment of personal or health information
- provides guidance on broad privacy issues and compliance
- conducts internal reviews about possible breaches of the PPIP Act and HRIP Act (unless the subject of the review is the conduct of the Privacy Contact Officer).

Please use the contact details below to contact the Privacy Contact Officer.

Our contact details

For further information about this plan, the personal and health information we hold, or if you have any concerns, please feel free to contact us.

Web:	www.ipc.nsw.gov.au
Email:	ipcinfo@ipc.nsw.gov.au
Phone:	1800 472 679
Mail:	GPO Box 7011 Sydney NSW 2001
Visit:	Level 17, 201 Elizabeth Street Sydney NSW 2000

Appendix A: about the privacy laws

This section contains a general summary of how we must manage personal and health information under the PPIP Act, the HRIP Act and other relevant laws. For more information, please refer directly to the relevant law, visit our website or contact us.

The PPIP Act and personal information

The PPIP Act sets out how we must manage **personal** information.

About personal information

Personal information is defined in s4 of the PPIP Act and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name, address, family life, sexual preferences, financial information, fingerprints and photos.

There are some kinds of information that are not personal information, e.g. information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public sector official. Health information is generally excluded here as it is covered by the HRIP Act.

Information protection principles (IPPs)

Part 2, Division 1 of the PPIP Act contains 12 IPPs with which we must comply. Here is an overview of them as they apply to us.

Collection

1. We collect personal information only for a lawful purpose that is directly related to our functions and activities.
2. We collect personal information directly from the person concerned.
3. We inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their personal information and any possible consequences if they decide not to give their personal information to us.
4. We ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.

Storage

5. We store personal information securely, keep it no longer than necessary and destroy it appropriately. We protect personal information from unauthorised access, use or disclosure.

Access and accuracy

6. We are transparent about the personal information we store about people, why we use the information and about the right to access and amend it.
7. We allow people to access their own personal information without unreasonable delay or expense.
8. We allow people to update, correct or amend their personal information where necessary.
9. We make sure that personal information is relevant and accurate before using it.

Use

10. We only use personal information for the purpose we collected it for unless the person consents to us using it for an unrelated purpose.

Disclosure

11. We only disclose personal information with people's consent unless they were already informed of the disclosure when we collected the personal information.

12. We do not disclose sensitive personal information without consent, e.g. ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

Exemptions to the IPPs

Part 2, Division 3 of the PPIP Act contains exemptions that may allow us not to comply with IPPs in certain situations. Here are some examples.

- We are not required to comply with IPPs 2-3, 6-8, or 10-12 if we are lawfully authorised or required not to do so.
- We are not required to comply with IPP 2 if the information concerned is collected in relation to a court or tribunal proceedings.

We do not use the other exemptions on a regular basis as they are not usually relevant to the work we do, however if we did use one we aim to be clear about the exemption we have used and our reasons for using it.

Privacy codes of practice and public interest directions can modify the IPPs for any NSW public sector agency. These are available on our website.

There are currently no codes of practice that are likely to affect how we manage personal information.

There are public interest directions that may allow us:

- not to comply with IPPs 2-3, 6-8, 10-12 if it is necessary in order for us to properly conduct investigations
- to be exempt from the IPPs when transferring enquiries to another NSW public sector agency
- to disclose personal information collected for research purposes.

The other public interest directions are unlikely to affect how we manage personal information.

Offences

Offences can be found in s62-68 of the PPIP Act.

It is an offence for us to:

- intentionally disclose or use personal information accessed in doing our jobs for an unauthorised purpose
- offer to supply personal information that has been disclosed unlawfully
- hinder the Privacy Commissioner or a member of staff from doing their job.

Public registers

The PPIP Act also governs how NSW public sector agencies should manage personal information contained in public registers (Part 6 – Public Registers).

Section 57 “Disclosure of personal information contained in public registers” states:

(1) The public sector agency responsible for keeping a public register must not disclose any personal information kept in the register unless the agency is satisfied that it is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.

(2) In order to enable the responsible agency to comply with subsection (1), the agency may require any person who applies to inspect personal information contained in the public register to give particulars, in the form of a statutory declaration, as to the intended use of any information obtained from the inspection.

Section 58 “suppression of personal information” states:

(1) A person about whom personal information is contained (or proposed to be contained) in a public register may request the public sector agency responsible for keeping the register to have the information

(a) removed from, or not placed on, the register as publicly available, and

(b) not disclosed to the public.

(2) If the public sector agency is satisfied that the safety or well-being of any person would be affected by not suppressing the personal information as requested, the agency must suppress the information in accordance with the request unless the agency is of the opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing the information.

(3) Any information that is removed from, or not placed on, a public register under this section may be kept on the register for other purposes.

As we neither hold nor maintain any public registers this section does not apply to us.

The HRIP Act and health information

The HRIP Act sets out how we must manage **health** information.

About health information

Health information is a more specific type of personal information and is defined in s6 of the HRIP Act. Health information can include information about a person's physical or mental health such as a psychological report, blood test or an Xray, or even information about a person's medical appointment. It can also include some personal information that is collected to provide a health service, such as a name and contact number on a medical record.

Health privacy principles (HPPs)

Schedule 1 to the HRIP Act contains 15 HPPs that we must comply with. Here is an overview of them as they apply to us.

Collection

1. We collect health information only for a lawful purpose that is directly related to our functions and activities.
2. We ensure that health information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.
3. We collect health information directly from the person concerned.
4. We inform people why their health information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their health information and any possible consequences if they decide not to give their health information to us.

Storage

5. We store health information securely, keep it no longer than necessary and destroy it appropriately. We protect health information from unauthorised access, use or disclosure.

Access and accuracy

6. We are transparent about the health information we store about people, why we use the information and about the right to access and amend it.
7. We allow people to access their own health information without unreasonable delay or expense.
8. We allow people to update, correct or amend their health information where necessary.
9. We make sure that health information is relevant and accurate before using it.

Use

10. We only use health information for the purpose we collected it for unless the person consents to us using it for an unrelated purpose.

Disclosure

11. We only disclose health information with people's consent unless they were already informed of the disclosure when we collected the health information.

Identifiers and anonymity

12. We do not use unique identifiers for health information, as we do not need them to carry out our functions.
13. We allow people to stay anonymous where it is lawful and practical.

Transfers and linkage

14. We do not usually transfer health information outside of NSW.
15. We do not currently use a health records linkage system and do not anticipate using one in the future. However if we did, we would not use one without people's consent.

Exemptions to the HPPs

Exemptions are located mainly in Schedule 1 to the HRIP Act, and may allow us not to comply with HPPs in certain situations.

An example of an exemption we may use is that we are not required to comply with HPPs 4-8, and 10 if we are lawfully authorised, required or permitted not to comply with them.

We do not use the other exemptions on a regular basis as they are not usually relevant to the work we do, however if we did use one we aim to be clear about the exemption we have used and our reasons for using it.

Health privacy codes of practice and public interest directions can modify the HPPs for any NSW public sector agency. These are also available on our website. Currently there are none that are likely to affect how we manage health information.

Offences

Offences can be found in s68-70 of the HRIP Act.

It is an offence for us to:

- intentionally disclose or use health information accessed in doing our jobs for anything else other than what we are authorised to
- offer to supply health information that has been disclosed unlawfully
- attempt to persuade a person from making or pursuing a request for health information, a complaint to the Privacy Commissioner or an internal review under the PPIP Act.

Other laws that affect how we comply with the IPPs and HPPs

This section contains information about the other laws that affect how we comply with the IPPs and HPPs.

Crimes Act 1900

Under this law we must not access or interfere with data in computers or other electronic devices unless we are authorised to do so.

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

Under this law people can apply for access to government information we hold. Sometimes this information may include personal or health information. If a person has applied for access to someone else's personal or health information we must consult with affected third parties. If we decide to release a third party's personal information, we must not disclose the information until the third party has had the opportunity to seek a review of our decision.

When accessing government information of another NSW public sector agency in connection with a review, the Information Commissioner must not disclose this information if the agency claims that there is an overriding public interest against disclosure.

Government Information (Information Commissioner) Act 2009 (GIIC Act)

Under this law the Information Commissioner has the power to access government information held by other NSW public sector agencies for the purpose of conducting a review, investigation or dealing with a complaint under the GIPA Act and GIIC Act. The Information Commissioner also has the right to enter and inspect any premises of a NSW public sector agency and inspect any record.

This Act also allows the Information Commissioner to provide information to the NSW Ombudsman, the Director of Public Prosecutions, the Independent Commission Against Corruption or the Police Integrity Commission.

Independent Commission Against Corruption Act 1988

Under this law we must not misuse information we have obtained in the course of doing our jobs.

Public Interest Disclosures Act 1994 (PID Act)

Under the PID Act people working within a NSW public sector agency can make a public interest disclosure (**PID**) to the Information Commissioner about a failure to properly fulfil functions under the GIPA Act.

We note that the definition of personal information under the PPIP Act excludes information contained in a public interest disclosure. This means that "personal information" received or collected under the PID Act is not subject to the IPPs or HPPs.

The PID Act requires that we must not disclose information that might identify or tend to identify a person who has made a PID. This plan will address how we protect the information we receive in relation to public interest disclosures.

State Records Act 1998 and State Records Regulation 2010

This law sets out when we can destroy our records. It also authorises the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies manage their records appropriately.

Appendix B: list of key privacy-related policies and procedures

Title	Issue covered	Author	Access
Strategic plan	Governance	IPC	IPC intranet / copy on request
Code of conduct	Governance	IPC	IPC website
Audit and Risk Committee Charter and Internal audit manual	Governance	IPC	IPC website
Public interest disclosures internal reporting policy	How to manage information received in relation to a public interest disclosure	IPC	IPC website
Service charter	Reinforces commitment to respecting the privacy of our stakeholders	IPC	IPC website
First aid policy	Incident reporting and health information	IPC	IPC website
First aid plan	Incident reporting and health information	IPC	IPC intranet / copy on request
Instrument of delegation (under s13 of the GIIC Act)	Delegation of who can give out information to parties of cases	IPC	OIC website
Email etiquette protocol	Staff not to BCC third parties inappropriately	DJ	IPC intranet
IPC office closure procedures	Make sure office is locked	IPC	IPC intranet
Acceptable use of the internet	Staff not to share computer logins or passwords	DJ	contact DJ
Use of mobile phones and blackberry devices	Staff have a duty of care to protect data on mobile phones	DJ	contact DJ
Emergency Procedures	Physical security	IPC	IPC intranet
Got an ethical problem – a guide for staff	Dealing with requests that may or may not be ethical. (could include privacy-related issues)	IPC	IPC intranet
Secondary Employment Policy Guidelines	Collecting personal information of staff re secondary employment	DJ	contact DJ
Casework and Compliance Manual	Information security for casework	IPC	Internal draft only
Guidelines for the Provision of Email	Autoforwarding emails and emailing confidential information	DJ	contact DJ
Use of Electronic Mail	Staff not to share computer logins or passwords	DJ	contact DJ
Sick Leave Policy and Guidelines	Collecting health information about staff	DJ	contact DJ
Family and Community Service and Carer's Leave Policy	Collecting personal and health information about staff and immediate family members	DJ	contact DJ