information and privacy commission
new south wales

IPC Privacy Management Plan

Updated October 2023

Who is this information for?	For all audiences and anyone seeking information on how the IPC manages privacy and personal information.
Why is this information important to them?	To explain how the Information and Privacy Commission NSW (IPC) manages personal and health information in accordance with NSW privacy laws.

Contents

The IPC reviews the information contained in this document every 12 months. The review will be conducted earlier if any legislative, administrative, or systemic changes affect how the IPC needs to manage personal information.

E-mail: ipcinfo@ipc.nsw.gov.au

Phone: 1800 472 679

Mail: GPO Box 7011 Sydney NSW 2001

1. Privacy Management Plan overview

A. Purpose

The purpose of this Privacy Management Plan (PMP) is to explain how the Information and Privacy Commission NSW (IPC) manages personal and health information in accordance with NSW privacy laws. This includes:

- *Privacy and Personal Information Protection Act 1998* (PPIP Act)
- *Health Records and Information Privacy Act 2002* (HRIP Act)

The PMP also explains who you should contact with questions about the information collected and retained by the IPC, how to access and amend your stored information and what to do if the IPC may have breached the PPIP or HRIP Acts.

Additionally, the PMP is used to train the IPC's staff about how to deal with personal information. This helps to ensure that the IPC complies with the PPIP Act, the HRIP Act and the GIPA Act.

Please refer to Appendix A for more information about NSW's privacy laws.

B. What the plan covers

This PMP includes requirements outlined in s33(2) of the PPIP Act including:

- information about how the IPC develops policies and practices in line with the state's information and privacy acts
- how the IPC disseminates these policies and practices within the organisation and trains its staff in their use
- the IPC's internal review procedures
- anything else the IPC considers relevant to the PMP in relation to privacy and the personal and health information it holds.

When preparing this PMP, the IPC also referred to its own privacy management plan's resources; the Guide to making privacy management plans, the Privacy Self-Assessment Tool and the Privacy management plan assessment checklist for agencies.

These resources are available on the IPC website.

C. Key definitions

Collection – (of personal information) the way in which the IPC acquires personal or health information, which can include a written or online form, a verbal conversation, a voice recording, or a photograph.

Disclosure – (of personal information) occurs when the IPC makes known to an individual or entity personal or health information not previously known to them.

Exemptions from compliance with Information Protection Principles (IPPs) – (general, specific and other exemptions) are provided both within the principles (and under Division 2 and Division 3 of Part 2 of the PPIP Act).

Health information – information or an opinion about a person's physical or mental health or disability, or a person's express wishes about the future provision of his or her health services or a health service provided or to be provided to a person; See the definition at S6 HRIP Act.

Investigative agencies – any of the following: Audit Office of NSW, the Ombudsman NSW, the Independent Commission Against Corruption (ICAC) or the ICAC inspector, the Law Enforcement Conduct Commission (LECC) or the LECC Inspector and any staff of the Inspector, the Health Care Complaints Commission, the Office of the Legal Services Commissioner, and Inspector of Custodial Services.

Law enforcement agencies – any of the following: the NSW Police Force or the police force of another State or Territory, the NSW Crime Commission, the Australian Federal Police, the Australian Crime Commission, the Director of Public Prosecutions of NSW or another State or Territory or of the Commonwealth, Department of Communities and Justice, Office of the Sherriff of NSW.

Personal information – 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. Exclusions to the definition of personal information are contained in s4(3) of the PPIP Act and includes health information; (see the definition at s4 PPIP Act and s4(3) PPIP Act and s5 of the HRIP Act).

Privacy principles – the Information Protection Principles set out in Division 1 of Part 2 of the PPIP Act and Health Principles set out in Schedule 1 of the HRIP Act. The privacy principles set out the minimum standards for all NSW public sector agencies when handling personal and health information. Within these principles lawful exemptions are provided.

Public register – a register of personal information that is required by law to be, or is made, publicly available or open to public inspection, whether or not upon payment of a fee.

Note: public register exemptions are provided for in clause 7 of the Privacy and Personal Information Protection Regulation 2014.

Privacy obligations – the information privacy principles and any exemptions to those principles that apply to the IPC, which is a public sector agency

Staff – any person working in a casual, temporary, or permanent capacity in the IPC, including consultants and contractors.

D. Data Breach Policy

Separate from this PMP, the IPC has a Data Breach Policy that sets out the IPC's procedures for managing a data breach, including the assessment and notification requirements for the Mandatory Notification of Data Breach Scheme under PIPPA.

2. About the IPC

A. IPC's responsibilities

The IPC is an independent agency that administers New South Wales legislation dealing with privacy and access to government information. Established on 1 January 2011, the IPC supports the Information Commissioner and the Privacy Commissioner in fulfilling their legislative responsibilities and functions.

The IPC is responsible for promoting compliance with these laws and legal instruments developed pursuant to the legislation and regulations including codes of practice:

- *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 2014*
- *Health Records and Information Privacy Act 2002* (HRIP Act)
- *Health Records and Information Privacy Regulation 2022*.

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.

Additionally, the IPC is responsible for:

- promoting and protecting privacy and information access rights in New South Wales
- providing information, advice, assistance and training for agencies and individuals on privacy and access matters
- reviewing the performance and decisions of agencies and investigating and resolving complaints related to public sector agencies, public and personal health service providers and some large organisations that deal with health information
- providing feedback on applicable legislation and relevant developments in the law and technology.

In order to fulfil its responsibilities, the IPC may collect personal and health information from its stakeholders, 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 (NGOs).

For more detailed information about the IPC and its legal framework, see the IPC website.

B. Policy and procedure development

The IPC is required to set out in this plan how policies and practices are developed to ensure compliance by the agency with the requirements of privacy legislation.

This plan sets out a number of specific elements of our privacy protection framework. Policies and practices are developed by:

- examining changes in the legislative, policy or operational environment for their impacts on the IPC's privacy management
- conducting regular reviews of privacy policies
- considering the privacy implications of changes to policies and systems for any procedural changes needed.

When developing new privacy management policies or procedures or amending them in a way that would change how personal and health information is managed, the IPC consults with the applicable parties to ensure compliance with the PPIP Act and HRIP Act.

Although the IPC is a separate agency, it is part of the Customer Service Cluster and it complies with relevant policies written by the Department of Customer Service (DCS), particularly concerning human resources, finance, procurement and information technology policies.

C. Promoting the PMP

The IPC promotes the principles of the PMP through its executive team, staff and public awareness.

Executive team

The IPC's executive team is committed to transparency and accountability in respect of the IPC's compliance with the PPIP Act and the HRIP Act.

The executive team reinforces transparency and compliance with these Acts by:

- endorsing the PMP and making it publicly available on its website
- identifying privacy issues when implementing new systems
- ensuring all staff are aware of sound privacy management practices.

IPC staff

The IPC ensures its staff is aware of and understand this PMP, particularly how it applies to the work they do. With this in mind, the IPC has written this plan in a practical way so staff members understand what their privacy obligations are, how to manage personal and health information in their work and what to do if they are unsure.

The IPC makes its staff members aware of their privacy obligations by:

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

When staff members have questions about how to manage personal and health information under the PMP, they may consult their manager or the IPC's Privacy Contact Officer (see Part E of this section).

Public awareness

The PMP is a guarantee of service to stakeholders on how the IPC manages personal and health information. Because it is central to how the IPC does business, this plan is easy to access on the IPC's website and easy to understand. For further information about the IPC's service commitments please see the IPC's Service Charter.

Additionally, the IPC is required to make this plan publicly available as open access information under the GIPA Act.

The IPC promotes public awareness of its PMP by:

- writing the plan in plain English
- publishing it on its 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 its privacy notices
- telling people about the plan when answering questions about how the IPC manages personal and health information.

D. External reviews, complaints and investigations

The IPC performs a number of activities with regard to privacy management compliance including:

- conducting external reviews of agency decisions on access applications for government information

- handling complaints about agency conduct under the *Government Information (Information Commissioner) Act 2009* (GIIC Act)
- investigating agency compliance with the GIPA Act
- handling public interest disclosures made to the Information Commissioner
- handling public interest disclosures made to the Privacy Commissioner
- overseeing internal reviews conducted by NSW public sector agencies in response to complaints about how they manage personal and health information under the PPIP Act and HRIP Act
- handling complaints about how NSW public sector agencies manage personal information under the PPIP Act
- dealing with complaints about how NSW public sector agencies and personal sector health providers managing health information under the HRIP Act
- investigating agency compliance with the PPIP Act and HRIP Act
- providing advice under the GIPA Act and Digital Restart Fund Act
- providing general advice to IPC stakeholders on privacy-related issues.

Sometimes, people may request 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 and GIIC Act. Anyone considering exercising their rights under the PPIP Act, HRIP Act, GIIC Act or GIPA Act anonymously is encouraged to contact the IPC to discuss their options.

E. Contacting the IPC

For further information about this plan, the personal and health information the IPC holds, or any other concerns, please contact the IPC.

The **IPC's Privacy Contact Officer is the Director Business Improvement**. You may contact the Privacy Contact Officer for information regarding:

- how the IPC manages personal and health information
- requests for access to and amendment of personal or health information
- guidance on broad privacy issues and compliance
- requests to conduct 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).

Contact the Privacy Contact Officer of the IPC at:

E-mail: ipcinfo@ipc.nsw.gov.au

Phone: 1800 472 679

Mail: GPO Box 7011 Sydney NSW 2001

Visit: Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

3. How the IPC collects personal and health information

The IPC collects and receives people's personal and health information in a variety of ways, in order to perform services and functions.

The collection of this information may be in writing, e-mail, through the IPC website enquiry form or the request for assistance form, over the phone, by fax, or in person at the IPC's office counter.

The IPC aims to tell applicants and its staff how it will manage their personal information when they seek our assistance, however, under the laws the IPC administers, it does not give people details of personal or health information it receives about third parties unless legally required to do so.

This section explains ways in which the IPC collects personal and health information during its business activities.

A. Enquiries

The IPC handles enquiries from its stakeholders about the right to government information and privacy protection in NSW.

These enquiries are made by people:

- over the phone (the IPC does not record telephone conversations, however, it does have a voicemail service)
- in writing (e-mail, letter, fax, online form)
- in person (at the IPC's office counter and at events).

The IPC decides what level of information is appropriate to be collected for each enquiry on a case-by-case basis, with the understanding that the details collected must contain enough information to be an accurate record of the issue and assistance given, but should not contain unnecessary personal and/or health information.

If someone writes to the IPC, a full copy of whatever is sent is generally kept by the IPC in its electronic document management system or in a hard copy file. However, if someone calls over the phone and gives a lot of background information, the IPC may decide not to record all the personal information if it is irrelevant to the enquiry. For example, an IPC staff member 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, in that respect, personal information may be provided that is unsolicited. The IPC recognises that some people may wish to remain anonymous, however, clear information regarding the consequences of remaining anonymous must be provided. For example, the IPC may be limited in considering personal factors under the GIPA Act or may not be able to properly investigate or consider the complaint or review application as the agency may not be able to respond in the absence of sufficient information about the matter. In these cases, it is up to the person who contacted the IPC to decide if they want to continue with the enquiry or not. If a person wishes to stay anonymous, the IPC only records the gender of the person who made contact.

The IPC's telephones will display the number of the person who called, except for private/silent numbers. Telephone conversations are not electronically recorded.

If someone has an enquiry that cannot be answered straight away, an IPC staff member will offer to take the person's name and telephone number so someone in the office can respond.

B. Complaints and reviews

Personal and health information is received by the IPC in many different forms related to the complaint and review processes including:

- from people seeking an external review or making a complaint to either the Information Commissioner or the Privacy Commissioner
- in notifications of internal reviews from the NSW public sector agencies conducting them
- from people sending their internal review application to the IPC to pass along to the NSW public sector agency conducting the internal review
- from people giving the IPC personal information about other people

- in response to IPC requests for people to send further personal and/or health information relating to a review or complaint
- in IPC file notes containing personal and/or health information
- from the Information Commissioner accessing information under the GIPA Act from NSW public sector agencies as it relates to the Commissioner's functions
- from the Information Commissioner entering the premises of NSW public sector agencies and accessing the agency's information and conducting investigations under the GIIC Act (will need abbreviation above)
- the Privacy Commissioner requiring a person or agency (and organisation under the HRIP Act) to provide information under the PPIP Act and HRIP Act to the Privacy Commissioner when it relates to the Commissioner's functions
- information received and collected by the IPC for NSW Civil and Administrative Tribunal (NCAT) proceedings, either at the proceedings or from submissions received from the parties.

C. Feedback and reports

Feedback

When people give the IPC feedback on the laws it administers, although not requested, 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 about other people. The IPC may ask for further personal information, but only to clarify the issue being raised.

The IPC stores this information on its computer network, in an electronic document management system and/or in hard copy files. Generally, the IPC does not disclose personal information obtained through feedback, except by consent or as allowed by law.

The IPC also publishes consultation papers to seek feedback on particular aspects of its laws. We do not ask for more information than what is helpful to us. The IPC may promote its consultation through various agencies, NGOs and media channels, however participation is voluntary.

Reports

The IPC provides guidance and advice to the public and agencies. One way of providing advice, guidance and assistance is to publish reviews and reports. The IPC seeks consent from people if any of their personal information is contained in a review or report prior to publication. If people do not consent to their personal information being published, the IPC may publish the report with their personal information de-identified.

Personal information is sometimes used to help us understand the context of the issue being raised and decide whether to write a report or bring an issue to the attention of the NSW Parliament, the Attorney General, Ministers, public or personal sector organisations or other relevant individuals.

When writing reports and making findings or submissions publicly available, the IPC does not identify people unless it relates to the purpose for which the information was collected; or has already sought the consent of the relevant people or notified them in advance of how the IPC would disclose the information provided.

The IPC relies on people to give accurate information and contact the IPC to amend it if necessary.

Surveys

The IPC conducts surveys on its services, advice and publications. These surveys may collect different kinds of demographic data. The IPC ensures any proposed survey or other kind of collection complies with the PPIP Act and HRIP Act.

Third party providers distribute these surveys on behalf of the IPC. The IPC ensures that these providers have appropriate privacy policies in place applying the relevant privacy principles and the information is collected in a secure environment. When people give the IPC responses to surveys, 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 about other people. The IPC may ask for further personal information, but only to clarify the issue being raised.

The IPC stores this information on its computer network, in an electronic document management system and/or in hard copy files. Generally, the IPC does not disclose personal information obtained through surveys, except by consent or as allowed by law.

D. IPC staff and recruitment

The IPC collects personal and/or health information from its staff members as part of the recruitment process. The IPC will never ask for more personal information than is required for that purpose.

Staff

During the recruitment process and throughout employment, information (including personal and/or health information) is collected from staff members for various reasons, such as leave management, unplanned absences, workplace health and safety and to help the IPC operate with transparency and integrity.

In the exercise of its functions the IPC collects and manages personal information about its staff including but not limited to:

- medical conditions and illnesses
- next of kin and contact details
- education
- contacting staff members about unexplained absences in accordance with the adopted Employee Welfare Check procedure
- performance and development information
- family and care arrangements
- secondary employment
- conflicts of interest
- financial information for payroll purposes
- employment history.

Information collected by the IPC is retained, to the extent necessary and managed securely.

Recruitment

When people apply for jobs at the IPC, they send us personal information, including their name, contact details and work history. The IPC gives this information to the convenor of the interview panel for that particular position (as stated in the job advertisement) in electronic or hard copy files.

The convenor of the panel does not use this personal information except for the purposes of the recruitment process. This can include sharing the information within the IPC business support, the relevant Commissioner(s) and members of the interview panel. Interview panels may include persons not employed by the IPC. Convenors store this information securely. After recruitment is finalised, convenors give all personal information back to the business support team to send to the human resources unit at DCS. 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 in order to commence employment at the IPC. These forms require further personal and health information, such as the applicant's 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 in order to collect data about the wider NSW public sector. Disclosing this information is voluntary.

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

E. Visitors and members of the public

When members of the public visit the IPC, a visitors' book is used to record the names of people who enter the office beyond the public area. This book is displayed on the front counter in the IPC's office.

The IPC collects this information for workplace health and safety purposes. The visitors' book is stored in accordance with IPC procedures.

F. Communications and stakeholder engagement

Subscriber, mailing and contact lists

The IPC keeps subscriber, mailing and contact lists that contain personal information from people who have asked to be included on these lists. No personal information is collected without consent and those who provide their information are advised as to how the IPC will manage it.

The information generally collected includes names, email addresses and in some cases, agency type. The IPC relies on people to provide accurate personal information and our staff are careful to enter the information correctly.

The main lists that collect and hold personal information are the:

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

All lists are kept separate from each other and each is used solely for the purpose intended. The IPC does not disclose individual email addresses when sending out bulk emails.

Anyone can subscribe or unsubscribe themselves from the newsletter list or contact the IPC to change their details. The IPC does not destroy these lists; they are kept as long as they remain current. Individual entries are deleted upon request or if an error message is received in response to an IPC communication.

Training sessions

When the IPC delivers training sessions to its stakeholders, it collects registration details of those who formally sign up to these public events. The details collected usually include names, email addresses, contact numbers and agency name, if applicable. It may also contain the personal views/opinions of participants. The IPC only uses this information to confirm numbers and communicate with participants about the particular event.

When providing in-house training for an agency, the IPC fills out an attendance list and provides it to the agency for their records. These lists contain names and positions only.

The information collected is stored electronically on a share drive, in paper form and with a third-party provider.

Health information is only collected if a participant has any special requirements or adjustments needed for the training session. This information is not retained after the event.

The IPC asks for feedback from training session participants and gives them the option of remaining anonymous. No names or contact details are requested. The IPC uses this feedback to improve its training sessions and materials. The IPC may publish collated feedback and comments but will not identify people.

Community outreach

The IPC occasionally holds community events or participates in events held by other agencies or organisations.

During these events, the IPC may collect general information such as the number of visitors to a stall, questions visitors asked, what resources were provided and general demographic information such as gender.

Depending on the event, the IPC may intentionally or unintentionally collect health information or sensitive personal information about someone. For example, if the IPC participates 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, the IPC seeks voluntary completion of surveys to help us identify current issues.

The IPC also seeks feedback from applicants on their experience with the commission in resolving their complaint, review, enquiry, or other matter.

Conferences and other events

The IPC hosts and participates in events including conferences and seminars. The IPC take the PPIP Act and the HRIP Act into consideration when organising such events and aims to inform people how the IPC will manage their personal and/or health information if it is collected, such as on registration forms.

Copies of presentations delivered by IPC representatives may be uploaded to a website for general use and accessed by conference organisers.

If an event management company is used to assist with delivering an event, the IPC will make sure it has appropriate privacy management practices in place. For more information, please refer to the section on Private sector companies, government agencies and contractors

Website publishing, photography, filming and media

The IPC owns and maintains the website: www.ipc.nsw.gov.au.

This website is used to promote Acts and publish resources to help our stakeholders understand and use the Acts. The IPC does not publish personal or health information on the website without permission.

Website data is stored on secure servers and on DCS managed networks.

The IPC may take photos of or film events that it holds or participates in and use the images for promotional purposes. The IPC will seek permission from people before taking photos or filming events and advise them how the IPC will manage the images and what they will be used for. Those who agree will be asked to sign a consent form. The IPC will respect the wishes of those who do not wish to be photographed or filmed.

The IPC stores photos and footage electronically on its computer network.

4. How information is managed by the IPC

This section describes how the IPC uses, discloses and stores personal and health information in alignment with its main types of services and functions.

A. Use of personal information

The IPC uses the information it collects to:

- conduct or oversee reviews and complaints
- 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.

The IPC makes sure personal information is accurate before using it. For example, the IPC would check contact details directly with a person to make sure the information is correct and will ask people to spell their names where necessary. This is to make sure information and correspondence is sent to the right person.

Personal information of IPC staff (see Section III D) is used by management, or via relevant reporting lines, specific to the staff member. The information may also be forwarded and disclosed to the human resources unit at the DCS or to other people management service providers supporting the IPC. Unless otherwise stated, the personal information collected by the IPC about its staff is used only for workforce management.

B. Disclosure of personal information

Enquiries

Personal information is used by the IPC only when dealing with enquiries related to that person. If the IPC receives more enquiries, a complaint, or review request from that person, it may look at past enquiries to get background information.

The IPC does not disclose information about a particular enquiry to anyone outside of its office without the consent of the enquirer.

Complaints and reviews

The IPC may discuss personal information with the relevant agency when conducting a review, complaint, or investigation. To undertake its functions the IPC discloses the name of review applicants to the agency that made the decision (see Section III). If a person does not give consent to the disclosure of their personal information to the relevant agency, the IPC will assess the complaint and determine how to deal with it.

The IPC includes relevant personal information in the reports it writes. The IPC generally sends these reports to the parties associated with the case and may publish the report to provide guidance to agencies and citizens (see Section III).

When the IPC is involved in NCAT cases, it may disclose personal information relevant to that particular case. It may also refer issues to other oversight bodies (see section III below).

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

The IPC is particularly careful when dealing with sensitive personal information, such as racial origin, health information, or sexuality.

Referrals to other oversight bodies

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

- an agency
- government ministers
- the NSW Ombudsman
- the Director of Public Prosecutions
- the Independent Commission Against Corruption
- the Law Enforcement Conduct Commission
- NSW Parliament and NSW Parliamentary Committees.

The Information Commissioner also has a Memorandum of Understanding with the NSW Ombudsman outlining how the two agencies share information with each other.

Additionally, the Privacy Commissioner has entered into an information sharing and complaint referral arrangement with the:

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

The NSW Privacy Commissioner has also 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 matter arising under another State, a Territory, or the Commonwealth; or 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.

The Privacy Commissioner may pursuant to s47 of the PPIP Act:

- 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
- 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.

GIPA Act

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

C. Storage and security of information

The IPC stores personal information electronically as hard copy files. The IPC practices a ‘clean desk’ approach, which means hard copy case files are secured at the end of the day or when not in use.

Sometimes, IPC staff members take files off-site in order to attend external reviews at the NCAT or the premises of other agencies. IPC staff members do not leave sensitive files unattended and do not let anyone else access them. Encrypted USB devices are used where possible.

The IPC records details of each enquiry on electronic enquiry registers and stores electronic and hard copies of written enquiries. No one other than the IPC staff can access these registers.

Systems, databases and information management

DCS provides services for the IPC with respect to information technology, finance, procurement and HR systems and support.

All of the IPC's electronic information is stored securely with the DCS shared service provider. The system complies with the DCS's Information Security Management System (ISMS) Policy. Under this policy:

- IPC servers are backed up daily
- IPC networks are secure and require individual logins and multifactor authentication
- IPC staff do not give out passwords to anyone or let anyone else use their computer login
- all IPC information is classified in line with Keyword AAA, a keyword thesaurus released by NSW State Archives and Records.

IPC retains its personal information in line with the disposal authorities approved by State Records, including FA 406. IPC considers and applies privacy compliance advice when considering and implementing new information management systems and software to ensure any new system complies with the PPIP Act and HRIP Act and will take reasonable steps to address any issues identified. A privacy impact assessment was undertaken for the IPC's GIPA Tool.

Case management databases and systems

Information collected as part of the investigation of complaints, reviews, enquiries or the giving of advice is held on the IPC's case management system, RESOLVE.

The databases are held on secure servers that are security compliant with the NSW Government Digital Information Security Policy.

IPC also manages the provision of an online case management tool for use by NSW agencies, known as the GIPA Tool.

The GIPA Tool is hosted on a cloud-based service operated by Salesforce, which is managed for the IPC by DCS. The IPC conducted a privacy impact assessment of the GIPA Tool in 2017 and it is managed in accordance with that assessment.

Physical security

Hard copy files are mainly located in the IPC office at Level 15, 2-24 Rawson Pl, Haymarket, Sydney NSW 2000. IPC staff have key card access to the office. Visitors cannot enter without permission. The IPC office is locked outside of business hours.

When not being used, hard copy files and sensitive information are securely stored. Secure printing is used by the IPC.

IPC staff members have unique user accounts and passwords to access our computer systems. In accordance with IPC's information security policy, our staff do not give out passwords to anyone or let anyone else use their computer login.

Older hard copy files are archived in a secure storage facility in compliance with the State Records Act 1998. For sensitive documents that need to be destroyed, the IPC uses locked bins from which the documents are securely destroyed.

Private sector companies, government agencies and contractors

The IPC may use private sector companies, contractors, or other government agencies for services. If these organisations or individuals have or are likely to have access to personal

information, the IPC ensures that personal and health information is managed in line with the PPIP Act, HRIP Act and information security policies. The IPC might do this by:

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

The IPC will also consider how a private sector company, agency or contractor will manage personal or health information they may have access to before engaging with them.

An external entity that may manage or collect personal information on behalf of the IPC includes:

- the DCS in providing information technology and human resources systems and support
- a secure shredding company in order to carry out the destruction of sensitive documents
- a marketing company that manages the IPC's mailing lists and newsletters
- temporary staff procured from providers under government contracts
- event management companies in order to host events and manage registrations
- independent contractors
- IT contractors.

5. How to access and revise your information

Everyone has the right to access the personal and/or health information the IPC holds about them. They also have the right to amend their own personal and/or health information the IPC holds, for example, updating their contact details.

The IPC is required to provide you with access to the personal and/or health information it holds and allow you to amend this information without excessive delay or expense.

There is no fee to access or amend your personal and/or health information.

This section explains how to request access to your own information via an informal or formal application.

A. Informal application

To access or amend your personal and/or health information, simply contact the IPC with your request.

To ensure your request is received by the proper IPC staff member or team managing your information, please follow these contact guidelines:

- Enquiries – contact the IPC's main enquiry line - 1800 472 679
- Case-related – contact the team or staff member handling the matter
- Newsletter subscriptions – use the IPC website to add or remove your details
- Staff information – speak with an IPC business support team member or contact the DCS's human resources department.

With an informal application, there is no need to put a request in writing. If necessary, an IPC staff member will ask you to verify your identity or, if applicable, make a formal application instead.

The IPC aims to respond to informal requests within **five working days**. After making your request, you will be informed if your request is likely to take longer than expected.

An IPC staff member will contact you to advise you of the outcome of the request. In some cases, particularly if it is sensitive information, you may be asked to make a formal application.

If you are not happy with the outcome of your informal request, you can submit a formal application.

B. Formal application

You can make a formal application at any time, without first making an informal request.

Address your formal application to the Privacy Contact Officer or Right to Information Officer by e-mail or post (see Contacting the IPC in Section II). The application should:

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

The IPC typically responds in writing to formal applications within **20 working days**. The IPC will contact you if your request is likely to take longer than expected. For additional information about the IPC's service goals, refer to the Service Charter on our website.

If you believe the IPC is taking an unreasonable amount of time to respond to your application for personal information, you are encouraged to contact the IPC to ask for an update or time frame.

If the IPC decides not to give access to or amend your personal or health information, the reason will be clearly explained to you in writing or over the telephone.

You also have the right to make a formal application to access information under the GIPA Act. For more information, please refer to the IPC website.

C. Accessing or amending other people's information

The PPIP Act and the HRIP Act gives people the right to access their own information; the Acts generally do not give people the right to access someone else's information.

However, s26 under the PPIP Act allows a person to give consent to the IPC to disclose his or her personal information to someone else that would not normally have access to it.

Likewise, under s7 and s8 of the HRIP Act, an 'authorised person' can act on behalf of someone else. The Health Privacy Principles (HPPs) also contain information regarding other reasons the IPC 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, in order to help find a missing person, or for compassionate reasons.

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

6. Your rights

A. Requesting an internal review

You have the right to seek an internal review under the PPIP Act if you believe the IPC has breached the PPIP Act or HRIP Act relating to your personal and/or health information. You cannot seek an internal review for a breach of someone else's privacy unless you are the authorised representative of the other person.

Applications for an internal review must be made in writing and within six months from when you first became aware of the breach. However, depending on circumstances, the IPC may also consider a late application for an internal review.

The internal review process

You can request an internal review by filling out the internal review form available on the IPC's website and sending it, along with any relevant information, to the IPC Privacy Contact Officer. Your submission can be made by email, fax, post, or in person at the IPC counter (see location details in Section II, Contacting the IPC).

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, as Chief Executive Officer, will appoint someone else within the IPC office to conduct the internal review.

The IPC aims 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 you of the progress of the internal review and if it is likely to take longer than first expected.

You can expect the Privacy Contact Officer to respond to you in writing within **14 calendar days** of deciding the outcome of the internal review. This is a requirement under Section 53 (8) of the PPIP Act.

If you disagree with the outcome of the internal review or are not notified of an outcome within **60 calendar days**, you have the right to seek an external review.

The Privacy Commissioner's role in internal reviews

An agency must notify the Privacy Commissioner an internal review is being conducted and also inform the Privacy Commissioner of the findings of the review and of the action proposed to be taken by the IPC in relation to the matter.

The Privacy Commissioner is entitled to make submissions to the agency with his or her view on the matter.

B. Requesting an external review

If you are unhappy with the outcome of the internal review conducted by the IPC or do not receive an outcome within 60 days, you have the right to seek an external review by the NSW Civil and Administrative Tribunal (NCAT).

You have **28 calendar days** from the date of the internal review decision to seek an external review under Section 53 of the *Administrative Decisions Review Act 1997 (NSW)*.

To request an external review, you must apply directly to the NCAT, which has the power to make binding decisions on an external review.

To apply for an external review or to obtain more information about seeking an external review, including current forms and fees, please contact the NCAT:

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

Phone: 1300 006 228

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.

C. Other ways to resolve privacy concerns

The IPC welcomes the opportunity to discuss any privacy issues you may have. You are encouraged to try to resolve privacy issues with the IPC informally before lodging an internal review.

You can raise your concerns with the IPC by:

- contacting the Privacy Contact Officer
- making a complaint directly to the Privacy Commissioner
- using the IPC's complaint process. For further information, view the IPC's Protocol for Handling Privacy Complaints.

Please keep in mind that you have **six months** from when you first 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. Please consider this time frame when deciding whether to make a formal request for internal review or continue with informal resolution.

D. Public interest disclosures

You have the right to make a public interest disclosure (PID) to the Information Commissioner about potential breaches of the GIPA Act, or a public interest disclosures to the Privacy Commissioner about potential breaches of the PPIPA or HRIPA Act, by government agencies.

The Information Commissioner, Privacy Commissioner, and the Director Legal Counsel and Regulatory Advice (DLCRA) are generally the only staff members in the IPC office who have access to and deal with public interest disclosures, although the PID Act 2022 also allows for any manager of a public official associated with the agency to deal with voluntary 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.

Generally, the IPC does not 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, Privacy Commissioner, or the DLCRA will speak with the complainant about courses of action.

E. Media enquiries

The IPC also deals with media enquiries. The IPC does not provide personal and/or health information to the media in response to their enquiries without consent.

7. Appendices

Appendix A: About NSW's privacy laws

This section contains a general summary of how the IPC 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 or contact the IPC or visit its website.

The PPIP Act and personal information

The PPIP Act sets out how the IPC 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 and address, details about their family life, their sexual preferences, financial information, fingerprints and photos.

There are some kinds of information that are not personal information, such as 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 the IPC must comply. Below is an overview of the principles as they apply to the IPC.

Collection

1. The IPC collects personal information only for a lawful purpose that is directly related to the IPC's functions and activities.
2. The IPC collects personal information directly from the person concerned.
3. The IPC informs people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. The IPC will 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. The IPC ensures personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.

Storage

5. The IPC stores personal information securely, keeps it no longer than necessary and destroys it appropriately. Personal information is protected from unauthorised access, use, or disclosure.

Access and accuracy

6. The IPC is transparent about any personal information that is stored, what it is used for and the right to access and amend it.
7. The IPC allows people to access their own personal information without unreasonable delay or expense.
8. The IPC allows people to update, correct, or amend their personal information where necessary.
9. The IPC makes sure that personal information is relevant and accurate before using it.

Use

10. The IPC only uses personal information for the purpose it was collected for unless the person consents to the information being used for an unrelated purpose.

Disclosure

11. The IPC will only disclose personal information with people's consent unless they were already informed of the disclosure when the personal information was collected.
12. The IPC does not disclose, without consent, sensitive personal information, such as 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 the IPC to not comply with IPPs in certain situations. Some examples include:

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

The IPC does not use the other exemptions on a regular basis as they are not usually relevant to the work or functions of the IPC. However, if another exemption was to be used, the IPC aims to be clear about the 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 the IPC website.

There are currently no codes of practice that are likely to affect how the IPC manages personal information.

There are public interest directions that may allow the IPC:

- making a complaint directly to the Privacy Commissioner
- not to comply with IPPs 2-3, 6-8, 10-12 if it is necessary 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 the IPC manages personal information.

Offences

Offences can be found in Part 8 of the PPIP Act.

It is an offence for the IPC to:

- intentionally disclose or use personal information accessed as a part of our work for an unauthorised purpose
- offer to supply personal information that has been disclosed unlawfully
- hinder the Privacy Commissioner or a staff member 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).

The IPC neither holds nor maintains any public registers, so this section of the PPIP Act does not apply to us.

The HRIP Act and health information

The HRIP Act sets out how the IPC 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, an X-ray, or even information about a person's medical appointment. It can also include personal information that is collected to provide to a health service, such as a name and contact number on a medical record.

Health privacy principles (HPPs)

Schedule 1 of the HRIP Act contains 15 HPPs that the IPC must comply with. Below is an overview of the principles as they apply to the IPC.

Collection

1. The IPC collects health information only for lawful purposes that are directly related to the IPC's functions and activities.
2. The IPC makes sure health information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.
3. The IPC collects health information directly from the person concerned.
4. The IPC informs people why their health information is being collected, what it will be used for and to whom it will be disclosed. The IPC will 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 the IPC.

Storage

5. The IPC stores health information securely, keeps it no longer than necessary and destroys it appropriately. Health information is protected from unauthorised access, use, or disclosure.

Access and accuracy

6. The IPC is transparent about the health information stored about people, what the information is used for and the right to access and amend it.
7. The IPC allows people to access their own health information without unreasonable delay or expense.
8. The IPC allows people to update, correct, or amend their health information where necessary.
9. The IPC makes sure the health information is relevant and accurate before using it.

Use

10. The IPC only uses health information for the purpose it was collected for, unless the person consents to the information being used for an unrelated purpose.

Disclosure

11. The IPC will only disclose health information with people's consent, unless they were already informed of the disclosure when the health information was collected.

Identifiers and anonymity

12. The IPC do not use unique identifiers for health information, as they are not needed to carry out the functions of the IPC.

13. The IPC allows people to stay anonymous where it is lawful and practical.

Transfers and linkage

14. The IPC does not usually transfer health information outside of NSW.
15. The IPC does not currently use a health records linkage system and does not anticipate using one in the future. However, if one were to be used, the IPC would not use one without people's consent.

Exemptions to the HPPs

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

For example, the IPC is not required to comply with HPPs 4-8 and 10 if the IPC is lawfully authorised, required, or permitted not to comply with them.

The IPC does not use the other exemptions on a regular basis as they are not usually relevant to the work of the IPC. However, if an exemption were used, the IPC aims to be clear about the 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 available on the IPC website. Currently, there are none that are likely to affect how the IPC manages health information.

Offences

Offences can be found in Part 8 of the HRIP Act. It is an offence for the IPC to:

- intentionally disclose or use any health information about an individual to which the official has or had access to in the exercise of his or her official functions
- offer to supply health information that has been disclosed unlawfully
- attempt to persuade an individual to refrain from making or to withdraw an application pursuing a request for access to health information or a complaint to the Privacy Commissioner or Tribunal
- by threat, intimidation, or false representation require another person to give consent or to do, without consent, an act for which consent is required.

Other applicable laws

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

Crimes Act 1900

Under this law, the IPC must not access or interfere with data in computers or other electronic devices unless it is authorised to do so.

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

The GIPA Act provides a mechanism to access your personal information or other information. An application can be made to the IPC to access information that the IPC holds. Sometimes, this information may include personal and/or health information.

If a person has applied for access to someone else's information, the IPC will take steps to consult with people who might have concerns regarding disclosure of their personal information. The IPC will provide notice of the decision to ensure that people who might want to object to the release of information have time to apply for a review of the decision to release information.

***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 or 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, IPC staff cannot misuse information obtained in the course of doing their jobs.

***Public Interest Disclosures Act 2022* (PID Act)**

The PID Act sets in place a system to encourage public officials to report wrongdoings. The NSW Information Commissioner is responsible for receiving complaints made as public interest disclosures about government information contraventions, as provided for under the PID Act. The NSW Privacy Commissioner is responsible for receiving complaints made as public interest disclosures about personal information privacy contraventions, as provided for under the PID Act.

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 the IPC to not disclose information that might identify or tend to identify a person who has made a public interest disclosure. This privacy management plan includes the IPC's procedures to protect the information received in relation to public interest disclosures.

For further information, refer to the IPC's Resources for Public Interest Disclosures.

State Records Act 1998* and *State Records Regulation 2015

This law sets out when the IPC can destroy its 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.

Document information:

Title:	IPC Privacy Management Plan
Business centre:	Systems and Corporate Services
Author:	Director, Business Improvement
Approver:	IPC CEO
Date of effect:	October 2023
Next review date:	October 2024
File reference:	D18/301288/DJ
Keywords:	Privacy management plan, corporate

Document history:

Version	Date	Reason for amendment
1.0	October 2018	Document created
1.1	January 2019	Document amended
2.0	October 2020	New version created
2.1	March 2021	Version updated
2.2	October 2023	Version updated