Privacy Management Plan

Purpose

IPART's Privacy Management Plan explains how IPART manages personal and health information in accordance with NSW privacy laws including the Privacy and Personal Information Protection Act 1998 (PPIP Act) and the Health Records and Information Privacy Act 2002 (HRIP Act).

This Plan explains how you can contact IPART with any questions relating to its management of this information, and what to do if you consider that IPART may have breached its legislative obligations relating to privacy.

Principles[1]

- IPART will only collect personal information for **lawful purposes** directly related to, and necessary for, the functions and activities of IPART.
- IPART will collect personal information **directly** from the individual, unless another individual is nominated and authorised, e.g. parent or guardian, or where assistance or support is required.
- The person to whom personal information relates:
  - will be **informed** by IPART of the collection, use, disclosure, whether it is required by law or voluntary, right of access and correction, and the name and address of collecting and holding agency;
  - has the **right to access** their personal information held by IPART; and
  - can request that IPART **amend** the information so that it is accurate, up to date and complete.
- IPART will take practical steps in all circumstances to ensure that personal information we collect, hold, or that is held on our behalf, is:
  - **accurate**, **up to date** and **complete** and that what we collect is both **reasonable** (not excessive) **and relevant** (not unreasonably intrusive);
  - **protected** (from loss, unauthorised access, disclosure, modification, and other misuse), and **kept no longer than necessary** for the purpose we collected it (subject to obligations under the State Records Act), before **secure disposal**.
  - accurate before we use it.

[1] Summary of principles in the Privacy and Personal Information Protection Act 1998 (NSW)

  - only used and disclosed for the **purpose(s)** for which it was collected unless the individual has consented to a different purpose, the use or disclosure is directly related to the purpose for which it was collected, there is a serious or imminent threat to life or health, or as otherwise required or authorised by law.
- We will not disclose personal information:
  - related to ethnicity or race, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless there is a serious or imminent threat to life or health;
  - **outside of NSW** unless there are comparable privacy laws in the jurisdiction.

Governance

Roles and responsibilities

Table 1 provides a summary of the roles and responsibilities for privacy at IPART.

Table 1 Roles and responsibilities

Role	Key responsibilities
Chief Executive Officer	• Ensure privacy principles are implemented across the business at IPART. • Ensure privacy breach response and risk management strategies are appropriate and effective. • Make the Privacy Management Plan publicly available. • Confirm support for privacy compliance in the Code of Ethics and Conduct.
Executive Leadership Team	• Ensure privacy principles are incorporated in IPART's policies and practices. • Review and endorse the Privacy Management Plan as required. • Ensure compliance with all IPART policies and procedures including Privacy Policy.
Privacy Officer	• Ensure the Privacy Management Plan is in place to support compliance with privacy legislation on an ongoing basis. • Advise and assist staff and the public in responding to requests for information. • Support the plan through awareness-building, skills development and user training.
Directors and Managers	• Read, understand and comply with the Privacy Management Plan. • Ensure all staff are provided with access to privacy training and comply with the Privacy Management Plan. • Identify privacy issues, risks and develop management strategies on reviews and projects. • Ensure appropriate procedures are in place to support compliance with this plan
Employees and contractors	• Act in accordance with the Privacy Management Plan and related policies and procedures • Be aware of and comply with all IPART policies including the Code of Ethics and Conduct, IPART Records Management and IPART User Security Awareness & Acceptable Use Policy. • Make sure that information is classified, labelled, and handled according to IPART and NSW guidelines. • Report any suspected or actual data breach to the Privacy Officer or Principal Risk Officer. • Seek advice when uncertain as to whether certain conduct may breach their privacy obligations • Report any suspected or actual security incident (including virus detection) to Service Desk, IT Contracts and Procurement Manager, or Principal Risk Officer.

If employees are uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice of the Privacy Officer.

How IPART collects personal information

IPART may collect personal and health information as part of our functions including:

- Subscriber, mailing and contact lists
- Submissions to our reviews
- Transcripts from public hearings
- Regulated service provider data
- Licence and accreditation applications
- Licence/accreditation compliance and monitoring (audits)
- Enquiries and media enquiries
- Complaints and feedback
- Public interest disclosures
- Staff and recruitment
- Visitor registration
- Government Information (Public Access) information requests
- IPART website visits - our website uses cookies to collect information.

How IPART uses and discloses personal information

Transparency is one of IPART's guiding principles. This means that we aim to ensure that the Tribunal's activities are well understood and that all stakeholders can participate as fully as possible in the Tribunal's processes. Stakeholder involvement is an important part of the Tribunal's processes to ensure that the Tribunal is aware of the range of viewpoints on the issues being considered. Refer to our open access information policy for more information.

Any personal information provided to IPART will be used and disclosed for the purposes for which we collected or received it, unless consent is received for another use or disclosure, in emergencies, or as otherwise required or authorised by law.

How IPART stores and protects personal information

Access to and use of personal information is restricted to authorised staff for the purpose of carrying out their official duties. Personal information that we collect in performing our pricing and regulatory functions, as well as our corporate functions, is stored in our records management system. All records containing personal information is stored and disposed of in accordance with the State Records Act 1998.

Our systems are hosted on secure platforms that are subject to ongoing assessment against NSW Cyber Security Policy with compliance reported in our Annual Report.

Service Providers

Where our service providers, use (e.g. NSW Government shared services), store (e.g. hosting at Government Data Centres) or dispose of personal information, they are bound by privacy provisions in our contracts. IPART regularly obtains assurance from key service providers including certification of their information security and quality management systems.

How IPART collects, uses and discloses personal information

In carrying out its functions IPART collects, receives, uses and discloses the following personal and health information:

Table 2

Collect / receive (IPP1)	Use	Disclose	IPP2	IPP3	IPP4
Communications and stakeholder engagement					
Subscriber, mailing and contact lists					
Our 'subscribe for updates' page on ipart.nsw.gov.au collects first name, last name, and e-mail address.	Relevant updates are e-mailed directly to subscribers through the website content management system.	We do not publicly disclose subscriber lists.	D	Y [a]	Y
Submissions					
Submissions to our reviews can be made via our online form or by post or fax using our cover sheet. IPART requests contact details including the name of the person providing the submission, the organisation that the person represents (if any) and an email or postal address.	IPART regularly seeks submissions from stakeholders to help us to understand their issues and views. We handle submissions received in accordance with IPART's submission policy. Submissions and summaries of submissions are provided to Tribunal members.	We disclose submissions as part of the relevant review on our website including name, position (if relevant) and organisation (if relevant) but only with the consent of the person making the submission (consent will be recorded: • on submission cover sheet, • on the online submission form; or • correspondence with the submitter (where it is not clear whether submitter consents to publishing personal details). IPART does not disclose e-mail or postal addresses when publishing submissions. If the submission is marked as 'anonymous' the submission will be published but not the person's name. If the submission is marked as 'confidential' all or part of the submission will not be published.	D	Y	Y

Collect / receive (IPP1)	Use	Disclose	IPP2	IPP3	IPP4
Regulated entity data					
Information collected during our investigation processes may include personal information. Any personal information is collected directly from the entities we regulate.	As part of our review process we may undertake research and analysis using regulated entity data.	We do not publicly disclose confidential information. We may use the information in our analysis and investigations, and formulating our recommendations. To the extent possible, we anonymise and aggregate information.	TP	NR	Y
Regulation and compliance					
In assessing licence or accreditation applications, we receive information on contacts, Chief Executive Officer and all Directors of the applicant company and any related company, including full name, date of birth, residential address and experience. As part of the licence or accreditation application assessment we collect company extracts from intermediaries which may contain additional information on Directors.	Company Director information received or collected during a licence or accreditation application assessment is used to conduct company searches to confirm that the named individual(s) are not disqualified individual(s) and to assess whether, among other things, organisational capacity to undertake the activities for which a licence is sought.	We publish licence applications on our website but only the full names of Contacts and Directors are disclosed with all other personal information redacted.	D TP	Y Y	Y Y
During selection of auditors and / or auditor selection panels, prospective Audit Panel members must complete Audit Panel Application Forms that include organisation, name, postal and e-mail address and phone numbers of contact persons and auditors.	IPART uses auditor information to assess the technical experience and qualifications of auditors.	IPART publicly discloses details of Audit Panel members including organisation, name, postal and e-mail address and phone numbers of contact persons.	D	Y [a]	Y
During compliance monitoring activities we may receive personal and health information related to safety incidents if an individual is involved.	IPART uses information gathered through incident reporting arrangements to determine and report on whether regulated entities are meeting their statutory obligations, and to identify risks and trends. IPART has entered into Memoranda of Understanding (MOUs) with a number of government, industry and consumer organisations to facilitate consultation and communication. These MOUs include provisions for the protection of information.		D / TP	N [b]	Y
Information that we collect during our audits may include personal information. Auditors may receive personal information directly from the regulated service provider as part of an audit.	Auditors use information gathered through audit arrangements to determine and report on whether regulated entities are meeting their statutory obligations, and to identify risks and trends. Protection of personal information by Auditors is covered by our Audit Service Panel Agreements: Energy Network Regulation, Water Industry Competition, and Energy Savings Scheme.		NA	NA	NA
Enquiries and media enquiries					
Our 'Enquiries' and 'Media enquiries' pages on ipart.nsw.gov.au collect first name, last name, e-mail address and contact number of anyone making enquiries.	Contact information related to enquiries is provided to the relevant IPART team member to respond to your enquiry.	No information related to individual enquiries and social media enquiries is published or otherwise disclosed by IPART.	D	Y [a]	Y

Collect / receive (IPP1)	Use	Disclose	IPP2	IPP3	IPP4
	Contact information related to media enquiries is provided to the Communications team to respond to the enquiry.				
Complaints and feedback					
When members of the public and other stakeholders make a complaint or provide feedback to IPART we collect their first name, last name, their preferred contact details, relevant facts / their opinion on the matter. Feedback or complaints can also be provided anonymously.	IPART handles complaints and feedback in accordance with IPART's External Complaints Handling Policy. If the complaint cannot be resolved on first contact it may re-assigned internally to an appropriate staff member.	No information related to individual complaints and feedback is published or otherwise disclosed by IPART. Statistical data on complaints is disclosed in our Annual Report.	D	Y [a]	Y
Public interest disclosures					
When employees or other public officials make a report of wrongdoing we collect their first name, last name, their phone, e-mail and postal address, relevant facts / their opinion on the matter. Public Interest Disclosures can also be provided anonymously. Confidentiality is dealt with according to IPART's Public Interest Disclosure Policy.	Reports of wrongdoing by employees and other public officials are handled in accordance with IPART's Public Interest Disclosure Policy including confidentiality provisions. All information related to Public Interest Disclosures are provided to, and retained by, our Disclosures Coordinator.	No information related to individual Public Interests Disclosure is published or otherwise disclosed by IPART. Statistical data on Public Interests Disclosure is disclosed to the NSW Ombudsman on a biannual basis and in our Annual Report.	D	Y [a]	Y
Staff and recruitment					
Through all phases of employment at IPART we collect personal information including: • Recruitment information including education, references and employment history • Employment contracts • Wage and salary entitlements • Personal details including name, data of birth, address and phone numbers • Emergency / next of kin contact name, address and phone numbers • Tax File Number and bank accounts • Performance reviews and development plans • Training and development activities • Sick leave and medical certificates • Family and care information • Leave and payroll data • Attendance and overtime records • Conflicts of interest • Restricted companies • Use of information technology resources.	Job applications, screening, interview and notification of successful candidates collected within the recruitment management system are distributed internally for use by the selection panel only. Candidate references and their contact details is used in the recruitment process and stored in the employee's personnel file. Employment, performance and development information is used by employees and their managers to set and monitor expectations. This information is maintained on employee personnel files in our records management system. Training registers are also maintained. Payroll, time records and leave information is used by employees and their managers to record and approve attendance. Medical certificates may be uploaded by employees to support leave of absence. This information is maintained on NSW government human resource and payroll systems.	IPART has outsourced some HR / Payroll functions. IPART only discloses personal information relating to staff and recruitment to its service providers under its service provider arrangements (refer *Service Providers*)	D	Y [a]	Y

Collect / receive (IPP1)	Use	Disclose	IPP2	IPP3	IPP4
	All conflicts and the agreed management strategy must be approved by the Chief Audit Executive and registered in IPART's conflict of interest register. IPART maintains a list of companies in which staff must not hold a pecuniary interest. On an annual basis all staff and Tribunal/Committee members must confirm in writing that they do not hold an undeclared pecuniary interest in any of the Restricted Companies. Declarations are maintained on employee personnel files.				
Vendor Master File (VMF) and Purchasing Card (PCard)	Employee bank account, name, address and phone number may be collected for EFT payment and retained in the VMF in SAP Finance system maintained by GovConnect. Completed PCard Application Form and Cardholder Agreement are sent to Westpac to issue a PCard. Name, Address, and Date of birth are sent to Westpac for employees to be setup in Corporate Online (Banking).	IPART has outsourced some finance functions. IPART only discloses personal information relating to its finance functions to its service providers under its service provider arrangements (refer *Service Providers*)	D	Y [a]	Y
Workers compensation: Where an employee injures themselves at work we collect information including Hazard & Incident reporting form, medical and return to work information.	We notify our insurer icare (EML) and establish a claim file with icare.	Personal information is disclosed to IPARTs insurer in accordance with the information protection principles and for the purposes of managing workers compensation cases. Statistical information in relation to WHS and Workers Compensation is disclosed in our annual report (i.e. no personal information/health information included).	D	Y [a]	Y
Visitors and members of the public					
Visitors to IPART either register themselves at reception or are pre-registered by IPART staff e-mailing contact details (name and company) to reception@customerservice.nsw.gov.au.	Use and disclosure of McKell building visitor information is subject to Department of Customer Service privacy provisions.		D	Y [a]	Y

Collect / receive (IPP1)	Use	Disclose	IPP2	IPP3	IPP4
Government Information (Public Access) Act 2009					
IPART collects information as part of GIPA information requests, complaints and correspondence including first name, last name, e-mail or postal addresses and other personal information specific to a particular matter.	GIPA information requests, complaints and correspondence received by IPART will be provided to a right to information officers to address with advice requested from our Legal Team (if required).	IPART is required to maintain a disclosure log under the GIPA Act. No personal information related to GIPA information requests will be disclosed by IPART. Statistical data on GIPA information requests is disclosed in our Annual Report.	D	Y [a]	Y
ipart.nsw.gov.au					
Visits to the IPART website are logged (see the Privacy Policy for our website for more information).	IPART website statistics may be used for internal purposes.	No personal information related to website visits will be disclosed to the public. Website statistics may be disclosed to other government agencies where requested.	D	Y	Y
Gifts and benefits register					
IPART's register of gifts and benefits records all but minor offers of gifts or benefits and whether it has been accepted or not.	The register is used to track and monitor offer and acceptance (including approval) of gifts and benefits.	IPART's gifts and benefits register will be subject to public disclosure on ipart.nsw.gov.au every 6-months in a manner that does not involve publishing individual employee names, but it will identify the organisation or company offering the gift or benefit.	D	Y [a]	Y
Pecuniary interests register					
Tribunal members must disclose any direct or indirect pecuniary interest in a matter being considered by the Tribunal and the interest appears to raise a conflict.	The register is used to track and monitor Tribunal member pecuniary interests in compliance with the IPART Act sch 3, cl 6.	The Pecuniary interests register for current Tribunal members is not on our website but is available for public to view on request. It is required to be available for inspection under the IPART Act.	D	Y [a]	Y

Not directly stipulated but limited collection i.e. first name, last name, e-mail, web page title i.e. media enquiries and PMP reasonably set out reason and use of collection.

Incident reporting relates to safety and reliability of electricity networks and water supply Safety

Note 1: Information Privacy Principle 1 (IPP1) - How the personal information IPART collects relates to our functions and activities

Note 2: IPP2 - Whether IPART collects personal information Direct from the individual or from a Third Party

Note 3: IPP3 - Does IPART adequately notify the individual that their personal information is being collected and why.

Note 4: IPP4 - Is the personal information being collected relevant, not excessive and is not an unreasonable intrusion.

Access and accuracy

This Privacy Management Plan provides general information on the personal and health information that IPART collects and holds.

IPART collects personal information directly from the individual or from regulated entities. We make every effort to check the accuracy of information received before we use it.

Under the PPIP Act, you have the right to access (and correct in certain circumstances) your personal information, if any, held by the IPART.

Staff members can access their own employment records. Managers have access to defined information about their employees for review and management purposes.

IPART's Privacy Officer will coordinate individual access to information we hold about them and facilitate any requests for amendment.

To access or correct your personal information, please make a written request addressed to the IPART Privacy Officer.

Public registers

We maintain the following publicly available registers:

Table 3 Publicly available registers

Register	Instrument	Publicly available
Pecuniary interest register	Schedule 2, clause 6 of the IPART Act	Register is not on our website, but is available for public to view on request.
Submissions received for each investigation	Section 22A of the IPART Act	Submissions can be made through ipart.nsw.gov.au for most reviews.
Electricity Access Agreements	Section 12E of the IPART Act	Electricity access arrangements available on ipart.nsw.gov.au
Transport Access Agreements	Section 12E of the IPART Act	Transport access arrangements available on ipart.nsw.gov.au
Gas reticulator authorisations	Section 18 of the Gas Supply Act .	List of current authorisations on website. Register is not on website but available for public to view on request.
Gas distributor licences	Section 46 of the Gas Supply Act	List of current licences on website. Register is not on website, but is available for public to view on request.
Electricity licences	Schedule 2, clause 10 of the Electricity Supply Act	Electricity licence register available on ipart.nsw.gov.au.
Greenhouse Gas Reduction Scheme registers	Section 162 of the Electricity Supply Act	Abatement certificate providers and NSW Greenhouse Abatement Certificates are available on the GGAS registry
Energy Savings Scheme registers	Section 162 of the Electricity Supply Act	Accredited Certificate Providers and Energy Savings Certificates are available on the ESS registry

Register	Instrument	Publicly available
Water Industry Competition Act licences	Section 20(1) of the Water Industry Competition Act	WICA Licence Register available on ipart.nsw.gov.au.

Note: These registers are still subject to the privacy protection principles.

Internal reviews and complaints

Complaints and feedback

Any complaints or feedback in relation to privacy can be directed to IPART's Privacy Officer or through IPART's External Complaints Handling Policy.

Internal review

If a person feels aggrieved by a contravention of an information protection principle by IPART, they are entitled to an internal review under the Privacy Act. The Act stipulates that an application for internal review must be:

- In writing (refer www.ipc.nsw.gov.au template).
- Addressed to IPART.
- Return addressed within Australia.

Lodged within 6 months of the alleged conduct coming to notice (s53(3)).

IPART will conduct an internal investigation to assess if we have complied with our privacy obligations – including advising and consulting with the NSW Privacy Commissioner. There is no fee. The investigation will be conducted by someone independent of the complaint.

We will keep the complainant and the NSW Privacy Commissioner informed of the progress of our review as well as the results.

You can also complain to the NSW Privacy Commissioner – refer 'How do I make a complaint?'.

External review

If you are unhappy with the result of the review (or it is not completed in 60 days) you have 28 days* to apply to the NSW Civil and Administrative Tribunal (NCAT) for a review of a decision about privacy or personal information. Refer Steps in a privacy matter.

Offences

All employees and contractors must familiarise themselves with their roles and responsibilities (refer Table 1) including ensuring they act in accordance with this plan and the PPIP Act and HRIP Act.

A breach of privacy is a breach of the code of ethics and conduct and may be subject to disciplinary action under the code of ethics and conduct.

Report any actual or suspected breach of an information protection principle immediately to the Privacy Officer or appropriate manager.

Under sections 62 and 63 of the PPIP Act it is an offence for an Officer to:

- Intentionally disclose or use personal information accessed in the exercise of official functions;
- Offer to supply personal information that has been disclosed unlawfully.

It is a criminal offence, punishable by up to two years' imprisonment, for any employee (or former employee) of IPART to intentionally use or disclose any personal information about another person, to which the employee has or had access in the exercise of his or her official functions, except as necessary for the lawful exercise of his or her official functions.

Privacy-related policies and procedures

Privacy is a mandatory consideration in policy development at IPART. We have the following policies governing storage, retention and disposal of information:

- IPART Code of Ethics and Conduct
- IPART Records Management Policy
- IPART User Security Awareness & Acceptable Use Policy
- IPART Information Security Policy
- IPART Submissions Policy

Promoting the PMP

The Privacy Management Plan is endorsed by the Executive Leadership Team and approved by our Chief Executive Officer before it is distributed by:

Internally

- Publishing the plan on the IPART Intranet, along with related policies and procedures, which is accessible to all staff.
- Highlighting the plan through an all staff e-mail whenever the plan is updated.
- Annual staff refresher training on Privacy
- Incorporated into other IPART policies and procedures
- Through the Privacy Officer providing advice and guidance as required.

Externally

- Publishing the plan on the IPART Internet and making it publicly available.
- Reporting on privacy issues in our annual report
- Confirming support for privacy in our Code of Ethics and Conduct.

Monitoring and review

This Plan is a managed document. Changes will be issued as a complete replacement document. This Policy will be reviewed, at a minimum every 2 years, or in response to material changes in the operating environment.

Implementation date: August 2020

Contact: Privacy Officer
Email: ipart@ipart.nsw.gov.au
Post: IPART, PO Box K35, Haymarket Post Shop, NSW 1240
Phone: 02 9290 8400

Definitions

Table 4 provides a glossary of key terms that are not explained elsewhere in this document.

Table 4 Definitions

Term	Definition
Collection	• Acquisition of personal or health information, which can include a written or online form, a verbal conversation, a voice recording, or a photograph.
Disclosure	• Makes known to an individual or entity outside the agency personal or health information not previously known to them.
Health information	• As defined in section 6 of the HRIP Act, health information is a specific type of 'personal information'. It includes but is not limited to: – information or an opinion about a person's physical or mental health, or a disability (at any time), such as a – psychological report, blood test or x-ray – personal information a person provides to a health service provider – information or an opinion about a health service already provided to a person e.g. attendance at a medical appointment – information or an opinion about a health service that is going to be provided to a person – a health service a person has requested, and – some genetic information
Personal information	• As defined in section 4 of the PPIP Act, personal information is information or an opinion that identifies a person (or that would allow a person's identity to be discovered). Personal information can include: – person's name, address, financial information and other details – photographs, images, video or audio footage, and – fingerprints, blood or DNA samples.
Privacy principles	• The minimum standards for all NSW public sector agencies when handling personal information. • See Division 1 of Part 2 of the PIPP Act

Term	Definition
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.

Title	Privacy Management Plan
Author	
Version	
Effective Date	August 2020
Owners	
Reference	
Approval	
Review Date	