Privacy Policy

Table of contents

1 Privacy and your rights

Members of the public are entitled to expect that we will treat any information provided you within the terms of relevant privacy responsibilities. For information about how the Department of Communities and Justice (the Department) deals with the personal informationof its customers, please visit our Privacy Management Plan. For information about your right to privacy and the Privacy and Personal Information Protection Act, please visit the website of the Privacy Commissioner.

The Department's website, along with its subsites, has developed a general privacy policy which is adhered to by all business units.

This Privacy Policy applies to all Departmental employees including permanent, temporary and casual staff, staff seconded from another organisation, and contingent workers including labour hire, professional services contractors and consultants.

2 Scope

This Privacy Policy outlines the personal information handling practices of the Department. It also describes how the Department deals with personal information. The Department's Privacy Policy provides a framework outlining how the Department manages personal and health information. We are committed to responsibly and properly managing the personal information we collect and protecting the privacy of our stakeholders, staff and members of the public.

The *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) applies to NSW public sector agencies including local councils and universities.

The specific legal obligations of the Department when collecting and handling your personal information are outlined in the PPIP Act and the HRIP Act, the Codes of Practice and Privacy Regulations.

3 What is Personal Information?

Personal Information is defined in the PPIP Act as information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from that information or opinion. Personal Information includes, for example, names, addresses, telephone numbers, email addresses, dates of birth and passport numbers.

Under the PPIP Act / HRIP Act some of the types of information about an individual that are not considered personal information, include:

- when it relates to a person who has been dead for more than 30 years;
- when it is contained in a publicly available publication;
- information arising out of a Royal Commission or Special Commission of

Inquiry;

- information contained in Cabinet documents.

3.1 What personal information do we collect?

Personal information is collected by the Department through:

- the Department's website;
- call centres - telephone enquiries;
- general e-mail enquiry accounts;
- correspondence received and forms completed by members of the public;
- individuals signing up to mailing lists;
- individuals who register for events; and
- feedback forms.

Personal information we collect is handled in accordance with the PPIP Act and the HRIP Act. The types of personal information collected include:

- names;
- addresses;
- telephone numbers;
- email addresses;
- dates of birth;
- IP addresses; and
- Other personal information as specified in this Policy.

More detailed information about how the Divisions within the Department handle personal information is set out in our Privacy Management Plan.

3.2 Personal Information provided by you

The Department aims to collect personal information about you directly from you. This may occur when you:

- Contact us to ask for information;
- Contact us for assistance with or consideration of an application specific to your circumstances;
- Inform or notify the Department about an issue;
- Provide submissions to the Department;
- Make a complaint;
- Ask for access to information held by the Department; or
- Apply for a job with the Department / provide referee reports.

We may collect your personal information from third parties, for example, your legal or other authorised representative or respondents to a complaint or inquiry.

We may also collect personal information from publicly available sources, for example, to enable us to contact stakeholders who may be interested in our work or in participating in our consultation.

Some agencies in the Department are lawfully authorised to collect information about you from third parties such as law enforcement agencies, investigative agencies or other public sector or private sector organisations when authorised by law, enabled by a privacy or health code of practice, public interest direction or with the consent of the individual.

When a division in the Department collects personal information as part of its functions and activities, the division will have its own privacy statement(s) and/or collection notices explaining how your personal information will be collected, used, stored and disclosed.

3.3 Automatic and indirect collection of personal information

The Department does not collect personal information and other data from you through the use of Cookies or other automated means including server logs. However, while we do not collect your personal information in this way, when you access the Department's website we will record non-personal information, for each page accessed. That is, the IP (Internet Protocol) address of the machine that accessed it.

We use Google Analytics to collect data about your interaction with the Department's website by using Google Analytics. We do this to improve your experience when using our website. The types of data we collect include:

- your device's IP address (collected and stored in an anonymised format);
- device screen size;
- device type, operating system and browser information;
- geographic location (country only);
- referring domain and out link if applicable;
- search terms and pages visited; and
- date and time when website pages were accessed.

This data is used to improve the services provided through the Department’s website. We will extract and publish this information about usage patterns from these records. For example, our usage reports will examine trends based on the following information – your server address,your top-level domain name (for example .com, .gov, .au, .uk etc), the date and time of visit to the site, the pages accessed, documents downloaded, the previous site visited, and the type of browser used and operating system.

On its websites the Department provides feedback facilities to allow users to provide input into the future development of its websites and comment on the provision of services.

Users are required to provide the Department with a name and an email address to enable a reply to any feedback. This information will only be used for the purpose for which it was provided. Your name and email address will not be added to any mailing list.

3.4 How we collect information indirectly to keep the Department secure

The Department will gather more extensive information relating to accesses to our website in the following circumstances:

- unauthorised attempts to access information that is not published on the Department's website pages;
- unauthorised tampering or interference with information published on the Department's website;
- unauthorised attempts to index the contents of the Department's website by other websites;
- attempts to intercept messages of other Department of Communities and Justice website users;
- communications that are defamatory, abusive, vilify individuals or groups or that give rise to a suspicion that a criminal offence is being committed; and
- attempts to compromise the security of the web server, breach the laws of the State of New South Wales or Commonwealth of Australia, or interfere with the enjoyment of the Department's website by other users.

Where required the Department may disclose this information to law enforcement agencies to investigate any contravention of laws that impact on the Department's security or functions.

3.5 Storage and Security

We take steps to protect the security of the personal information we hold from both internal and external threats by:

- regularly assessing the risk of misuse, interference, loss, and unauthorised access, modification or disclosure of information;
- providing mandatory and regular targeted privacy training to the various agencies in the Department;
- where appropriate, employees and service providers are required to sign confidentiality agreements and enter into information sharing agreements regarding access to and the use of personal information held by the Department; and

- Divisions in the Department are encouraged to develop robust governance frameworks in relation to the handling of personal information.
- The Department's Data Breach Response Plan provides guidance and direction on responding to data breaches that may impact the personal information held by the Department.

Information collected by the Department is also stored securely in accordance with StateArchives requirements. More detailed information on our storage and security standards and practices is available in our Privacy Management Plan.

Access by Departmental employees, contractors or other authorised parties to personal information held by the Department is determined by role and the need for access. Unauthorised access to and use of personal information is taken seriously as it constitutes a data breach and disciplinary or other action may be taken by the Department.

Personal Information is only retained for as long as necessary and securely destroyed or de-identified once it is no longer required by law. Further information about records disposal authorities relevant to agencies in the Department is set out in theDepartment's Privacy Management Plan and by the State Records Authority.

3.6 Social Networking Services

We use social networking services such as Twitter, Facebook, LinkedIn and YouTube to communicate with the public about our work. When you communicate with us using these services we do not collect your personal information.

3.7 Anonymity

We will require your name, contact information and sufficient information relating to your inquiry in order to carry out most of our functions in order to provide you with a service.

Where possible we will allow you to interact with us anonymously or by using a pseudonym. For example, if you contact an enquiry line with a general question you will not be required to provide your name unless we need your personal information to adequately handle your question.

3.8 Use of Personal Information

The personal information you provide to the Department will be used for the primary purpose for which you provided it and any secondary purposes where it is directly related to that primary purpose. Detailed information in relation to the use of information collected by the agencies in the Department is detailed in the Privacy Management Plan.

3.9 Disclosure of Personal Information

The Department will disclose your personal information in the following circumstances:

- where you have already been made aware of the disclosure to third parties;
- the disclosure is required to be made to an investigative or law enforcement agency (as defined in the PPIP Act)'
- the disclosure is authorised or required by law;
- the disclosure to a third party is necessary to prevent or lessen a serious and imminent threat to the life or health of you or another person; or
- with your consent.

More specific information about disclosure of information is contained in the Department's Privacy Management Plan and privacy statements relevant to each agency's functions and activities.

To protect the personal information we disclose we may, where appropriate:

- enter into a contract or Memorandum of Understanding (MOU) requiring the service provider to only use or disclose the information for the purposes of the contract or MOU; and / or
- include special privacy requirements / clauses in the contract or MOU, where necessary.

3.10 Quality of Personal Information

To ensure the personal information we collect and use is accurate, up-to-date and complete we:

- record information in a consistent format;
- where necessary, confirm the accuracy of information we collect if the information is collected from a third party or a public source; and
- promptly add updated or new personal information to existing records.
- provide you with avenues to contact the Department to update us with any changes to your contact details or your circumstances.

We also take reasonable steps to review the quality of personal information before we use or disclose it to third parties as set out in the Privacy Management Plan.

3.11 How can I access or amend my personal information?

Under the PPIP Act and the HRIP Act you have a right to ask for access to personal information / health information we hold about you. You also have a right to ask that we correct that personal / health information if you believe it is incorrect.

You can ask for access to your personal information or for a correction to that personal information by contacting us. If you ask, we must give you access to your

personal information unless there is a lawful reason preventing that access. We must take reasonable steps to correct personal information if we consider it is inaccurate or incorrect, unless a law prevents us from doing so. Medical reports or specialist reports cannot be amended as they are specialist point in time reports. If we refuse to correct your personal information, you can ask us to associate with it (for example, attach or link) a statement that you believe the information is incorrect and why you hold this belief.

You also have the right under the *Government Information (Public Access) Act 2009* (GIPA) to request access to documents that we hold. Excluded information of some agencies, as set out in Schedule 2 of the GIPA Act (e.g. the Office of the Legal Services Commissioner, NSW Trustee and Guardian) cannot be accessed under the GIPA Act. Further information about accessing information under the GIPA Act is available on the Access to Information page.

3.12 Data Breach

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* is a Commonwealth Act which established a Notifiable Data Breaches (NDB) scheme. NDB applies to the Department as a tax file number recipient (TFN) as the Department holds Tax File Numbers for employment and other business related purposes. A TFN recipient is any person who is in possession or control of a record that contains TFN information.

A Notifiable Data Breach is a data breach that is likely to result in serious harm to any person to whom the information relates. A data breach may occur where personal information held by the Department is lost or subject to unauthorised access or disclosure.

Further information in relation to the scheme is accessible through the following links:

- entities covered by the NDB scheme
- identifying eligible data breaches

A data breach or allegation of a breach relating to any agency within the Department will be promptly notified to Legal. Legal will co-ordinate a response in line with the Department's Data Breach Response Plan to deal with the incident/alleged breach. Responding to a data breach notification may include targeted inquiries about the nature and extent of the breach, notification of affected individuals, notifying the NSW Privacy Commissioner and facilitating remedial action.

NSW data breach obligations

On 28 November 2022, the *Privacy and Personal Information Protection Amendment Act* 2022 was assented to. The amendments to the PPIP Act will come into effect 12 months following assent, from 28 November 2023.

They aim to strengthen privacy legislation in NSW by:

• creating a Mandatory Notification of Data Breaches (MNDB) Scheme which will

require public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm

• applying the PPIP Act to all NSW state-owned corporations that are not regulated by the *Commonwealth Privacy Act* 1988

• repealing s117C of the *Fines Act* 1996 to ensure that all NSW public sector agencies are regulated by the same mandatory notification scheme.

The MNDB Scheme will require agencies to satisfy other data management requirements, including to maintain an internal data breach incident register, and have a publicly accessible data breach policy.

3.13 Complaints

If you would like to make a complaint regarding an alleged breach of privacy by the Department of Communities and Justice you may do so in writing to the Open Government, Information and Privacy Unit, Legal. Further information on how to lodge a complaint, the internal review application form and assistance on how to complete an internal review application form, is available through the following links:

- Privacy Internal Review application form
- Procedures for conducting Internal Reviews

Any comments or enquiries regarding this Policy and any concerns or complaints about the information handling practices of the Department of Communities and Justice can be addressed to the Office of the General Counsel, Department of Communities and Justice:

Open Government Information and Privacy Unit
Email: infoandprivacy@dcj.nsw.gov.au
Telephone: (02) 9716 2662

Alternatively, complaints or concerns about your privacy may be directed to the NSW Privacy Commissioner:

Email: ipcinfo@ipc.nsw.gov.au

Phone: 1800 472 679

Mailing address: Level 17, 201 Elizabeth Street Sydney 2000

4 Related legislation and documents

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

5 Document information

Document name	Privacy Policy
Applies to	Department of Communities and Justice
Replaces	NA
Document reference	Where is this saved e.g. in TRIM
Approval	December 2017
Version	2.0
Commenced	December 2017
Due for review	2023
Policy owner	Open Government, Information and Privacy Unit

6 Support and advice

Who can people go to if they need more advice?

Business unit	Open Government, Information and Privacy Unit
Email	infoandprivacy@dcj.nsw.gov.au