Privacy Policy

Table of contents

1 Purpose

This Policy outlines:

- the personal information handling practices of the Department of Communities and Justice (DCJ)
- our commitment to responsibly managing the personal information we collect to ensure the privacy of our stakeholders, staff and members of the public.

2 Definitions

Term	Definition
DCJ's Data Breach Policy	DCJ's Data Breach Policy is a policy that provides an overview of DCJ's procedures in relation to containing, assessing, managing, notifying and reporting, eligible data breaches in accordance with the Mandatory Notification of Data Breach Scheme.
Health information	Health information is a class of personal information and includes information or opinions about the health or disability of an individual and or a patient's wishes about future healthcare. It also includes information collected in connection with the provision of a health service (Section 6 of the *Health Records and Information Privacy Act 2002*).
Health Privacy Principles	The legal obligations which NSW public sector agencies and private sector organisations, must abide by when they collect, hold, use and disclose a person's health information (Schedule 1 of the *Health Records and Information Privacy Act 2002*).
Information Protection Principles	The legal obligations which NSW public sector agencies must abide by when they collect, store, use or disclose personal information (Sections 8-19 of the *Privacy and Personal Information Protection Act 1998*).
Personal information	Information or an opinion about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion (section 4 of the *Privacy and Personal Information Protection Act 1998*).
Privacy Management Plan	A document that outlines how DCJ complies with its obligations under the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002* (section 33 of the *Privacy and Personal Information Protection Act 1998*).

Mandatory Notification of Data Breach Scheme	Means the scheme under Part 6A of the *Privacy and Personal Information Protection Act 1998* for assessing and notifying of eligible data breaches.
NSW Privacy Commissioner	Means the Privacy Commissioner appointed under the *Privacy and Personal Information Protection Act 1998*.
State record	Has the same meaning as in the *State Records Act 1998*.

3 Scope

The following persons must comply with this policy:

- all DCJ permanent full time, part time, trainee and temporary employees
- any other persons authorised to access DCJ's information systems and assets including consultants, third party suppliers, vendors and hosted/managed service providers.

4 Policy Statement

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

Members of the public expect DCJ to treat any personal and health information provided by them, in accordance with the Information Protection Principles outlined in the PIPP Act, and the Health Privacy Principles in the HRIP Act.

DCJ's Privacy Management Plan supports this Policy by explaining how DCJ complies with its obligations under the PPIP Act and HRIP Act.

5 What is personal and health 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, but is not limited to: names, addresses, telephone numbers, email addresses, dates of birth and passport numbers.

Health information is defined in the HRIP Act as personal information that is information or an opinion about a person's health, disability or the provision of health services.

Some types of information about an individual **are not** considered personal information, for example:

- information that relates to a person who has been dead for more than 30 years
- when the information is contained in a publicly available publication

- information arising out of a Royal Commission or Special Commission of Inquiry
- information contained in Cabinet documents.

5.1 What personal information do we collect?

The types of personal information that may be collected by DCJ includes, but is not limited to, information about:

- you, including your name, date of birth and contact details
- your circumstances such as your corrective services history, employment history or welfare
- your family such as any children, partners, carers or dependents
- your interactions with us such as payments or services we provide, or any applications, feedback or complaints you have made
- how you use our online services including any portals and or social networking pages
- as specified in this Policy.

Further details about how the Divisions within DCJ handle personal information is set out in our Privacy Management Plan.

5.2 How we collect your personal information

Personal information is collected by DCJ through a number of means, including:

- DCJ's website(s)
- 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
- feedback forms
- our social media pages.

5.2.1 Collection of personal information from you

DCJ aims to directly collect personal information from you 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 DCJ about an issue
- provide submissions to DCJ

- provide feedback or make a complaint
- ask for access to information held by DCJ
- apply for a job with DCJ and or provide referee reports
- interact with DCJ through social networking services.

5.2.2 Collection of personal information from third parties

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

Some divisions in DCJ 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
- a Public Interest Direction waives or changes the requirements for a public sector agency to comply with an Information Protection Principle
- the individual consents.

When a division in DCJ 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.

5.2.3 Automatic collection of personal information

DCJ may collect personal information and other data from you through automated means, for example, webpages you visit, online forms you complete and any searches you conduct.

DCJ uses Google Analytics to collect information about your interaction with DCJ's website to improve user experience. The types of information we collect includes:

- your device's Internet Protocol (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
- date and time when website pages were accessed.
- the pages accessed and any documents downloaded.

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

Users are required to provide DCJ 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.

5.2.4 How we collect information to keep DCJ secure

DCJ 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 DCJ's website pages
- unauthorised tampering or interference with information published on DCJ's website
- unauthorised attempts to index the contents of DCJ's website by other websites
- attempts to intercept messages of other DCJ website users
- communications that are defamatory, abusive, vilify individuals or groups, and or that give rise to a suspicion that a criminal offence is being committed
- attempts to compromise the security of the web server, breach the laws of the State of New South Wales or the Commonwealth of Australia, or interfere with the enjoyment of DCJ's website by other users.

Where required, DCJ may disclose this information to law enforcement agencies to investigate any contravention of laws that impacts DCJ's security or functions.

5.3 Storage and Security

We take steps to protect the security of 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 and cyber security training to various business units in DCJ
- 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 DCJ

- divisions in DCJ are encouraged to develop robust governance frameworks in relation to the handling of personal information
- frequently reviewing our suite of information management and security policies

DCJ's Data Breach Policy provides further guidance and direction on how we respond to data breaches where there is an unauthorised access, disclosure or loss of personal information held by DCJ.

Information collected by DCJ is stored securely in accordance with State Records Act requirements. Detailed information on the storage, security standards and practices are available in DCJ's Privacy Management Plan.

Access by DCJ employees, contractors or other authorised parties to personal information held by DCJ 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; disciplinary or other action may be warranted in those circumstances.

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 DCJ is outlined in the Privacy Management Plan and State Records NSW.

5.4 Social Networking Services

DCJ uses social networking services such as Twitter, Facebook, LinkedIn and YouTube to communicate with the public about our work. We collect your personal information when you interact or communicate with DCJ using these services.

5.5 Anonymity

We will require your name, contact information and sufficient information relating to your enquiry in order to carry out most of our functions, including the provision of services offered by DCJ.

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 manage your question.

5.6 Use of personal information

The personal information you provide to DCJ will be used for the primary purpose for which you provided it, including any secondary purposes that is directly related to that primary purpose, unless an exception or exemption applies. Detailed information in relation to the use of personal information collected by DCJ is available in the Privacy Management Plan.

5.7 Disclosure of personal information

DCJ may 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
- with your consent.

Specific information about the disclosure of personal information relevant to each Division's functions and activities is contained in the Privacy Management Plan.

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
- include special privacy requirements and or clauses in the contract or MOU (where necessary).

5.8 Quality of personal information

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

- 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
- promptly add updated or new personal information to existing records
- provide you with avenues to contact DCJ 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.

5.9 How can I access or amend my personal information?

Under the PPIP Act and the HRIP Act, you have a right to access personal and or health information we hold about you. You also have a right to ask DCJ to correct your personal and health Information if you believe it is incorrect.

You can request access to, or a correction of, your personal information by contacting us. If you ask, we must provide access to your personal information unless there is a lawful reason preventing access.

We must take reasonable steps to correct personal information if we consider it is inaccurate or incorrect, unless a law prevents us from amending the information. Medical reports or specialist reports cannot be amended as they are point in time reports. If we refuse to correct your personal information, you may ask us to associate the subject information with a statement provided by you that outlines why you believe the information is incorrect.

You also have rights under the *Government Information (Public Access) Act 2009* (the GIPA Act) to request access to information held by DCJ. Visit DCJ's Access to Information page for further details about accessing information under the GIPA Act.

5.10 Mandatory Notification of Data Breach Scheme

Part 6A of the PPIP Act establishes the Mandatory Notification of Data Breach (MNDB) Scheme.

Under the MNDB Scheme, NSW public sector agencies are required to notify the NSW Privacy Commissioner of an eligible data breach. Affected individuals will also be notified unless an exception applies. An eligible data breach occurs if there is:

- an unauthorised access, disclosure or loss of an individual's information held by an agency, and
- a reasonable person would conclude that the unauthorised access, disclosure, or loss would likely result in serious harm to an individual to whom the information relates.

Other key obligations for NSW public sector agencies under the MNDB Scheme include:

- Preparing and publishing a Data Breach Policy.
- Containing and assessing suspected data breaches.
- Establishing and maintaining an internal register for eligible data breaches.
- Maintaining and publishing a Public Notification Register for any public data breach notifications issued by the agency.

5.10.1 Managing Data Breaches

A data breach or an alleged data breach relating to any division in DCJ must be promptly notified to the Open Government, Information and Privacy Unit, DCJ Legal (OGIP). OGIP will co-ordinate and manage the data breach, in conjunction with DCJ's Cyber Security Team (where necessary), in accordance with DCJ's Data Breach Response Plan.

Responding to a data breach may include targeted inquiries about the nature and extent of the breach, notification to affected individuals, notifying the NSW Privacy Commissioner and facilitating remedial action.

5.10.2 Commonwealth data breach scheme

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* is a Commonwealth act which established a Notifiable Data Breaches (NDB) scheme. NDB applies to DCJ as it holds Tax File Numbers (TFN) 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 NDB 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 DCJ is lost or subject to unauthorised access or disclosure.

Specific information relating to the entities covered by the NDB scheme is available at the Office of the Australian Information Commissioner.

5.11 Complaints

Any comments, complaints or enquiries regarding this Policy and or concerns regarding DCJ's information handling practices can be addressed to OGIP:

Email: infoandprivacy@dcj.nsw.gov.au
Telephone: (02) 9716 2662

Further information on how to lodge a complaint, including an internal review, is outlined in DCJ's Privacy Management Plan.

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: GPO Box 7011, Sydney NSW 2001

6 Related legislation and documents

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *State Records Act 1998*

7 Document information

Document name	Privacy Policy
Applies to	DCJ
Replaces	N/A
Document reference	D24/3324374
Approval	January 2025
Version	4.0
Commenced	January 2025
Due for review	30 June 2026
Policy owner	Open Government, Information and Privacy Unit

8 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