Privacy Management Plan

December 2022

This Privacy Management Plan has been adapted from the Department of Communities and Justice Privacy Management Plan.

Contents

Introduction/Overview

Multicultural NSW is committed to respecting the privacy rights of clients, employees and members of the public.

Purpose

The *Privacy and Personal Information Protection Act 1998* (the "PPIP Act") provides for the protection of personal information and for the protection of the privacy of individuals. The *Health Records and Information Privacy Act 2002* (the "HRIP Act") protects the privacy of health information.

The PPIP Act sets out 12 Information Protection Principles (IPPs) relating to personal information, and the HRIP Act sets out 15 Health Privacy Principles (HPPs) relating to health information. These principles set the privacy standards that NSW public sector agencies are expected to follow when dealing with personal information. The principles cover information collection, storage, use and disclosure of personal and health information.

Scope

The PPIP Act (Section 33) requires all public sector agencies to prepare a Privacy Management Plan that covers:

- policies and practices that ensure compliance with the requirements of the PPIP Act and the HRIP Act
- how these policies and practices will be communicated to our staff and stakeholders
- the proposed internal review procedures

This Privacy Management Plan shows how we intend to comply with the requirements of privacy legislation in NSW. We also want people to know how we manage personal information.

This plan outlines how we will incorporate Information Protection Principles and Health Privacy Principles into our everyday functions.

Roles and Responsibilities

All employees are required to comply with the PPIP Act and the HRIP Act. This plan is designed to assist employees to understand and comply with their obligations under the PPIP Act and the HRIP Act. It is also intended to provide the community with information about how we meet our privacy obligations. Advice and support for employees is available from the Director, People and Corporate in relation to privacy compliance, rights, and obligations.

All employees are responsible for:

- familiarising themselves with and complying with the Privacy Management Plan when dealing with personal and health information,
- identifying whether new projects are likely to raise privacy issues and consulting Director, People and Corporate where appropriate,
- identifying and raising privacy concerns with their Manager or Director,
- participating in privacy training to improve their knowledge and awareness of privacy obligations.

Promoting privacy awareness

We take our privacy obligations very seriously and undertake a range of initiatives to ensure our employees, contractors and members of the public are informed of our privacy practices and obligations under the PPIP Act and the HRIP Act. We promote privacy awareness and compliance by:

- publishing and promoting this plan on our intranet and website,
- incorporating privacy information in our induction program and in the modules for Code of Conduct and Fraud and Corruption awareness,
- publishing and promoting all privacy policies on our intranet,
- enabling staff to access a dedicated privacy page on the Department of Communities and Justice intranet that centralises privacy resources for our employees and that provides information about what to do if employees are unsure about a privacy issue,
- delivering periodic face-to-face and online training across different business areas,
- investigating allegations of breaches of privacy and implementing recommendations made from finalised investigations,
- assessing privacy impacts of new projects or processes from the outset,
- working with senior executives to endorse a culture of good privacy practice,
- educating the public about their privacy rights and our obligations (for example, providing privacy information on forms that collect personal and health information).

Definition and exclusions

The PPIP Act is concerned with 'personal information'. Personal information is defined in the PPIP Act as being "any information or opinion about a person whose identity is apparent or can be reasonably ascertained from the information or opinion."
While the definition of 'personal information' is very broad, there are some important exceptions to the definition. The exceptions that are most relevant to the Agency is information:

- arising out of a Royal Commission or Special Commission of Inquiry
- contained in Cabinet documents
- about an individual's suitability for appointment or employment as a public sector official arising from the exercise of specific statutory law enforcement powers such as telephone interception, controlled operations, and witness protection.

These exceptions do not interfere with the confidentiality or sensitivity of these types of information and exemptions from the requirements of the PPIP Act do not mean that other policy or statutory requirements, such as the confidentiality of Cabinet documents, can be disregarded.

Main classes of information collected

A general description of the information commonly held by the Agency includes:

- employee personnel records
- community contact information
- administrative records
- correspondence
- submissions and consultation responses
- interpreting and translating records
- grant records
- award records

Information Protection Principles

Collection

The Agency takes active measures to ensure that the collection of personal and health information is relevant, not excessive, and is not an unreasonable intrusion into the affairs of an individual by regularly reviewing privacy collection notices to ensure they accurately reflect the collection of personal information relevant to business needs.

Generally, when we collect personal and health information, the information is collected directly from the individual. However, the individual may authorise the collection of their information from another person

When collecting personal and health information from individuals, we give a privacy notice to the individual to whom the information relates. Section 10 of the PPIP Act and Schedule 1 Clause 4(1) of the HRIP Act sets out what is required in this notification. This includes the purpose for collection, intended use and recipients, whether the information is required, and the individual's right and method of access and amendment to that information. Where health information is collected from someone other than the individual, the individual will be notified as soon as possible after the collection unless an exemption or exception applies.

Employee records

For various reasons, such as leave management, workplace health and safety and operational requirements, we must keep employee records including:

- documents related to the recruitment process
- payroll, attendance and leave records
- banking details and tax file numbers
- training records
- worker's compensation records
- workplace health and safety records
- records of gender, ethnicity and disability of employees for equal opportunity reporting purposes
- medical conditions and illnesses
- next of kin and emergency contact
- secondary employment
- conflicts of interests

This information is collected directly from employees and will be managed in accordance with the provisions of the PPIP Act and the HRIP Act.

Business records

We maintain business records that contain personal information including contact details for public officials in other government entities, as well as other third-party organisations.
Health information may also be collected and retained consistent with our obligations under the HRIP Act and Contracts with other government and third-party entities and individuals may include personal information or health information but is only collected in accordance with the privacy principles. This may include individuals engaged as contractors rather than ongoing employees.

Accuracy of personal information

To ensure that personal information is correct, checks are undertaken on the accuracy of personal information that is collected by verifying this information directly with the person providing the information. Completed forms are checked to ensure legibility, completeness, and accuracy.

Disclosure

We collect, use, store and disclose the personal and health information of individuals for several reasons for the purpose of fulfilling our functions and activities. The terms 'use' and 'disclosure' are not defined in privacy legislation however case law has developed to give them different meanings under the Act.

In general, to 'use' information means to handle information that has been collected, and requires some administrative action or consequence for example, an employee using a person's personal information to prepare a report. To 'disclose' information means to give information collected by us to a person or body outside of our Agency for example if we were to provide information to the NSW Police Force.

When considering whether to use personal information or health information we hold, we must consider whether:

- the proposed use is consistent with the purpose for which it was collected, or
- the proposed secondary use is directly related to the purpose of collection, or
- the individual has consented to use of their personal information for that purpose, or
- it is necessary to prevent or lessen a serious and imminent threat to the life or health of a person.

We can use the information for the proposed purpose if any of the above circumstances apply. One way for us to ensure that personal or health information has been used or disclosed lawfully is by obtaining consent. For consent to be valid, it must be voluntary, informed, specific, current, and given by a person who has the capacity to give it.

It is important to note that we have the discretion to disclose personal information and health information to law enforcement agencies without the consent of the individual concerned when a search warrant, subpoena, summons, or statutory order has been issued upon us.

Restricted personal information

The following categories of personal information are given more stringent protection under section 19 of the PPIP Act:

- an individual's ethnic or racial origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- sexual activities

These categories of information are only collected when required for a particular function or activity and may only be disclosed if it is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or of another person.

Storage

We will take reasonable security safeguards to protect personal and health information from loss, unauthorised access, use, modification or disclosure, and against all other misuse. We will ensure personal and health information is stored securely, not kept longer than necessary, and disposed of appropriately.

We use a variety of information management systems to manage our storage and security obligations including paper-based filing systems, and electronic records forming part of secure computerised databases. Strict rules are followed for storing personal information and health information in all its formats in order to protect personal information and health information from unauthorised access, loss or other misuse. Only those employees who need to know particular personal information or health information in order to carry out their work can have access to it. Personal information and health information, both paper-based and electronic media, must be stored securely in our electronic systems and protected from unauthorised access and alteration.

Personal information and health information must be kept only as long as it is necessary for the purposes for which it may lawfully be used. When it is no longer needed, the personal information or health information must be destroyed using a secure waste destruction service (for paper-based documents) and formal deletion processes for electronic documents and data.

Personal and health information held in our records can only be disposed of in accordance with the NSW State Records Act 1998 and the relevant disposal authorities.

Data breaches

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* establishes a Notifiable Data Breaches scheme (NDB). NDB applies to the Agency as a tax file number (TFN) recipient as we hold TFN's 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 us is lost or subject to unauthorised access or disclosure.

Access

The PPIP Act and the HRIP Act both establish a right of access to information for individuals about themselves. Individuals are entitled to know whether information about them is held by us, the nature of the information, the main purposes for which it is used, and how they can gain access to it, including a right of correction if details are not correct.

Informal Requests

A person wanting to access or amend their own personal or health information can make a request by contacting the relevant business unit that manages their information. Generally, this request does not need to be made in writing, however a written request may be required to ensure the request is accurately understood and actioned. If a person is not satisfied with the outcome of their informal request, they can make a formal application.

Formal Application

A person can make a formal application for access to personal information under the HRIP Act or the PPIP Act by requesting it directly from the relevant business area in writing or by seeking advice about how to do this by contacting the Agency directly. Formal applications should include:

- The applicant's name and contact details
- Whether the application is made under the HRIP Act or the PPIP Act
- What personal or health information is to be accessed or amended

The Agency will aim to respond to the formal application in 30 working days, depending on the volume of information requested, and will advise the applicant approximately how long the application will take to process, particularly if it may take longer than expected.

Where an application to access information held by us includes personal information about another person, an access application should be made under the Government Information (Public Access) Act 2009 (GIPA Act). Further information about GIPA is available from
The Privacy Officer
Multicultural NSW
PO Box 618
Parramatta NSW 2124
Email: info@multicultural.nsw.gov.au

Privacy Complaints and Internal Review

Any person can make a privacy complaint by applying for an 'internal review' of the conduct they believe breaches the HRIP Act or the PPIP Act.

A person can also discuss any concerns with the Privacy Officer or email info@multicultural.nsw.gov.au

An internal review is a process by which we manage formal, written privacy complaints about how we have dealt with personal information or health information. All written complaints about privacy are considered to be an application for internal review, even if the applicant doesn't use the words 'internal review'. If you would prefer to resolve your privacy concern informally, please let us know when you contact us. We may also endeavour to deal with your complaint informally, with your consent, without the need for the formalities of an investigation.

Your rights of internal review

An application for internal review should:

- be in writing to the Agency
- specify an address in Australia at which you can be notified after the completion of the review
- provide as much detail as possible about the suspected privacy breach to be reviewed

The Internal Review follows the process set out in the Information & Privacy Commission's internal review checklist. When the internal review is completed, you will be notified in writing of:

- the findings of the review
- the reasons for those findings
- the action we propose to take
- the reasons for the proposed action (or no action), and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal (NCAT).

We are also required to provide a copy of our draft internal review report to the Privacy Commissioner and consider any submissions made by the Privacy Commissioner.
We will keep the Privacy Commissioner informed of the progress of the internal review and will provide a copy of the finalised internal review report. Further information about the internal review process is available on the IPC website.

Timeframes

You must lodge your request for internal review within six months from the time you first became aware of the conduct that you think breached your privacy. We will acknowledge receipt of an internal review and will aim to complete the internal review within 60 calendar days. We will contact you if the review is likely to take longer than 60 days to complete.

We will contact you in writing within 14 calendar days of completing the internal review. If the internal review is not completed within 60 days, or if you are unhappy with the outcome of the internal review you have a right to seek a review of the conduct by the NCAT.

You have 28 calendar days from the date of the internal review decision to seek an external review. To request an external review, you must apply directly to the NCAT. To apply for an external review or to obtain more information about seeking an external review, including current forms and fees, please contact NCAT:
Website: http://www.ncat.nsw.gov.au/
Phone:1300 006 228 or (02) 9377 5711
Visit/post: Level 9, John Maddison Tower,
86-90 Goulburn Street,
Sydney NSW 2000

Other ways to resolve privacy concerns

We welcome the opportunity to discuss any privacy issues you may have. You are encouraged to try to resolve privacy issues with us informally before lodging an internal review.

Complaints to the Privacy Commissioner

Individuals have the option of complaining directly to the Privacy Commissioner if you believe that we have breached your privacy. The Privacy Commissioner's contact details are:
Office: NSW Information & Privacy Commission
Level 17, 201 Elizabeth Street Sydney NSW 2000
Post: GPO Box 7011
Sydney NSW 2001
Phone: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au

Monitoring and Review

We will review this plan every 12 months. We will review the plan earlier if any legislative, administrative or systemic changes impact our management of personal and health information.

Document Control

NAME/TITLE	Privacy Management Plan
APPROVED BY	Joseph La Posta, Chief Executive Officer
DATE APPROVED	TBC
DATE EFFECTIVE	TBC
CONTACT OFFICER	Director People and Corporate
ISSUED TO	All Staff