

Privacy Management Plan

Number	SR-P23/5	Version	1.1
Category	Policy	Subject	Governance
Issued by	Executive Director	Approval Date	05.04.2023
Authorised by	Executive Director	Issued Date	06.04.2023
Distribution	External	Review Date	05.04.2025

Purpose

The purpose of this Privacy Management Plan (PMP) is to outline how the State Records Authority NSW (State Records NSW) collects and manages personal and health information in accordance with NSW privacy laws. This PMP provides staff and contractors with necessary knowledge and skills to manage personal and health information appropriately.

Background

The *Privacy and Personal Information Act 1998* (PIIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) regulate the way public sector agencies collect, store, use and disclose personal and health information. The PIIP Act protects personal information through 12 Information Protection Principles (IPPs) and the HRIP Act has 15 Health Protection Principles (HPPs). Under the legislation individuals have the right to complain about the possible misuse of personal information through non-compliance with the IPPs or HPPs.

Scope

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

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

This PMP outlines how the PMP is implemented at a local level throughout the course of business activities.

1. About State Records NSW

1.1 State Records NSW responsibilities

State Records NSW is the NSW Government's records management authority. State Records NSW is a statutory body with responsibilities and functions established by the *State Records Act 1998*:

- to oversee recordkeeping by public offices of NSW, including determining standards and providing advice
- to identify State records that have enduring value and should be retained as State archives.

State Records NSW performs its functions by:

- setting and monitoring standards for the creation, management, and disposal of State records;
- providing practical advice, guidance, and training to NSW public sector bodies in all aspects of records management;
- identifying State records which should be retained as State archives
- providing permission to dispose of State records after minimum retention requirements have been met.

In order to fulfil its responsibilities, State Records NSW may collect personal and health information from NSW public offices and members of the public.

1.2 Duty of Confidentiality

State Records NSW employees handle, have access to and inspect the records of other NSW Government organisations. This means that they regularly have access to records that contain personal information. The State Records Act recognises this and places a special duty of confidentiality on them (**see Appendix 2**).

1.3 Policy and procedure development

State Records NSW 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.

Policies and practices are developed by:

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

State Records NSW consults with the applicable stakeholders when amending or developing new privacy management policies or procedures.

Although State Records NSW is a separate agency, it is part of the Museums of History NSW (MHNSW) and State Records NSW staff agency and it complies with relevant policies written by the MHNSW, particularly concerning human resource, finance, procurement and information technology policies.

1.4 Promoting the PMP

State Records NSW promotes the principles of the PMP through its executive team, staff and public awareness.

1.5 Executive Director and Managers

State Records NSW is committed to transparency and accountability in respect of its compliance with the PPIP Act and the HRIP Act.

The Executive Director and Managers 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.

1.6 State Records NSW staff

State Records NSW makes its staff members aware of their privacy obligations by:

- publishing the PMP in a prominent place on its intranet and website
- including the PMP in induction packs and offering training quarterly or as required
- highlighting and promoting the PMP at least once a year (e.g. during Privacy Awareness Week).
- Requiring new staff to undertake privacy training as part of the onboarding and induction process
- Requiring staff to review the Code of the Conduct annually.
- Requiring staff to sign an additional confidentiality agreement, filed in their personnel file.

When staff members have questions about how to manage personal and health information under the PMP, they may consult their manager or supervisor.

1.7 Public awareness

The PMP is a guarantee of service to stakeholders on how State Records NSW manages personal and health information. Because it is central to how State Records NSW does business, this plan is easy to access on its website and easy to understand. For further information about the State Records NSW service commitments please see the [Service Charter](#).

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

State Records NSW 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
- telling people about the plan when answering questions about how State Records NSW manages personal and health information.

2. How State Records NSW collect personal and health information

State Records NSW collects and receives people's personal and health information in a variety of ways to perform services and functions. The collection of this information may be in writing, e-mail, website enquiry forms, over the phone, or in person.

This section explains ways in which State Records NSW collects personal and health information during its business activities.

2.1 Enquiries

State Records NSW handles enquiries from its stakeholders about recordkeeping in public offices.

These enquiries are made by people:

- over the phone (State Records NSW does not record telephone conversations, however, it does have a voicemail service)
- via Microsoft Teams application
- in writing (email, letter, online form)
in person (at events or meetings).

State Records NSW 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 State Records NSW, a full copy of whatever is received is generally kept by State Records NSW in its records system. However, if someone calls over the phone and gives a lot of background information, State Records NSW may decide not to record all the personal information if it is irrelevant to the enquiry. For example, the State Records NSW staff member might make a general note, such as 'concerned about records containing personal information kept by a public office' without recording details about the personal information itself.

The provision of any personal information is entirely voluntary and, in that respect, personal information may be provided that is unsolicited. State Records NSW recognises that some people may wish to remain anonymous and only records that the enquiry came from either the member of the public or the private sector, public office under the NSW jurisdiction or from another jurisdiction.

State Records NSW telephones will display the number of the person who call, except for private/silent numbers. Telephone conversations are not electronically recorded.

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

2.2 Complaints

Personal information is received by State Records NSW in many different forms related to the complaint process including:

- People making a complaint about State Records NSW services, products or staff member.
- Members of the public making a complaint about a public office's recordkeeping policies, procedures or practices.
- Information received and collected by State Records NSW in handling complaints or submissions received from public offices.

2.3 Feedback and reports

Feedback

When people give State Records NSW feedback on the law 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. State Records NSW may ask for further personal information, but only to clarify the issue being raised.

State Records NSW stores this information on its computer network, in its records system and/or in an electronic file. Generally, State Records NSW does not disclose personal information obtained through feedback, except by consent or as allowed by law.

State Records publishes consultation papers to seek feedback on particular aspects of State Records Act 1998, regulation, standards, codes of best practice and authorities. State Records NSW do not ask for more information than what is helpful to us. State Records NSW may promote its consultation through various agencies or social media channels, however participation is voluntary.

Reports

State Records NSW provides guidance and advice to NSW public offices and the public. One way of providing advice, guidance and assistance is to publish reports and case studies. State Records NSW seeks consent from people if any of their personal information is contained in a report or case study prior to publication. If people do not consent to their personal information being published, State Records NSW may publish the report with their personal information de-identified.

When writing reports and making findings or submissions publicly available, State Records NSW 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 State Records NSW would disclose the information provided.

State Records NSW relies on people to give accurate information and contact the State Records NSW to amend it if necessary.

2.4 Surveys

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

Survey respondents may decide to provide us personal information, such as contact details, personal opinions, stories, experiences and backgrounds. They may also provide us personal information about other people. State Records NSW may ask for further personal information, but only to clarify the issue being raised.

State Records NSW stores this information on its computer network, in its records systems and/or in electronic files. Generally, State Records NSW does not disclose personal information obtained through surveys, except by consent or as allowed by law.

2.5 Staff and recruitment

MHNSW administers the human resources function of State Records NSW.

MHNSW collects personal and/or health information from its staff members as part of the recruitment process and human resources function. MHNSW 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) may be collected from staff members for various reasons, such as leave management, unplanned absences, workplace health and safety and to help State Records NSW and/or MHNSW operate with transparency and integrity.

MHNSW administers the human resources function of State Records NSW.

In the exercise of its functions State Records NSW and/or MHNSW may collect and manages personal and health information about its staff including but not limited to:

- medical conditions and illnesses
- next of kin and contact details;
- education;
- performance and development information;
- secondary employment;
- family and care arrangements
- conflicts of interest
- financial information for payroll purposes; and
- employment history.

Information collected by State Records NSW and/or MHNSW is retained to the extent necessary and managed securely.

Recruitment

When people apply for jobs at State Records NSW, they do so through the *iworkforNSW* portal for all NSW Government positions, and will send personal information, including their name, contact details and work history.

This information is given to the convenor of the interview panel and panel members for that role (as stated in the job advertisement) in electronic or hard copy files. All panel members sign a confidentiality agreement for each recruitment panel they participate in. Information relating to successful applicants is

retained as part of the employee's personnel file. Unsuccessful applications are destroyed in accordance with the requirements of General Retention and Disposal Authority – Administrative Records (GA28).

Successful applicants are invited to fill out various forms to commence employment at State Records NSW. 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. They may also include pre-employment medical information.

These forms also encourage people to provide sensitive personal information, such as racial and cultural information to collect data about the wider NSW Public Sector. Disclosing this information is voluntary.

These forms are sent to the People and Culture team at MHNSW to be used for employment purposes, such as payroll and setting up personnel files. The People and Culture team at MHNSW keeps copies of this information in secure storage areas.

3. Communications and stakeholder engagement

As part of administering the State Records Act, State Records NSW may share contact information of its stakeholders to the MHNSW.

3.1 Subscriber, mailing and contact lists

State Records NSW 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 State Records NSW will manage it.

The information generally collected includes names, email addresses, telephone numbers and position titles. State Records NSW relies on people to provide accurate personal information and 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 For The Record newsletter to those who have requested subscription
- chief executives, corporate records managers, and other key contacts in NSW public offices – to email compulsory recordkeeping requirements or to provide access to specific services
- contacts in other archives institutions and similar organisations

All lists are kept separate from each other and is used solely for the purpose intended. State Records NSW does not disclose individual email addresses when sending out bulk emails and does not provide subscriber details to third parties without permission. Anyone can subscribe or unsubscribe themselves from the newsletter list or contact State Records NSW to change their details.

The lists are retained as long as they are required and current.

This information is stored in applications, such as Mailchimp and Salesforce, records system and computer networks, only accessible to State Records NSW using a unique password.

3.2 Boards and advisory committees

State Records NSW maintains contact details of members of its Board and advisory committees. Information about Board members includes private as well as work contact details. Contact details of members of the Board and advisory committees is used to support the administration of meetings. Private contact details of Board members are collected to enable them to be contacted in urgent cases or emergencies.

3.3 Forums, webinars and clinics

Participant information

When State Records NSW holds forums, webinars and clinics to its stakeholders, it collects registration details of those who formally sign up to these 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. State Records NSW only uses this information to confirm numbers and communicate with participants about the event.

When providing face-to-face events, State Records NSW requests participants to check their participation against an attendance list. For unregistered participants, they are asked to provide their names, email addresses and agency names using an attendance list. These lists contain names, email addresses and agency name.

During these events, State Records NSW may collect general information such as the number of participants, questions participants asked, what resources were provided and general demographic information such as location of the public office.

State Records NSW asks for feedback from participants to improve its events and services. Participants are given an option to remain anonymous or to provide State Records NSW their names or contact details if they wish to be contacted for further feedback. State Records may publish collated feedback and comments but will not identify people.

The information collected is stored electronically on a computer network, in paper form or with an online application or tool.

Presenter information

Copies of presentations delivered by State Records NSW representatives and agency representatives may be uploaded to a website for general use. The presentations may contain the presenters' names, email addresses, and in some cases position titles. The presenters are given the option to publish or not to publish their presentations, including their names and contact details.

Online Recordings

In most cases, State Records NSW may record forums, webinars and clinics held online. The convenor will inform the participants when recording commences and ends.

Depending on the online application used to facilitate the online event, a notification is sent to all participants when recording commences and ends, and provision of consent is provided by staying connected to the online event.

The recordings are used for general use and access by participants. State Records NSW use the recordings to promote best practice recordkeeping and to help identify issues or future enhancements to its service offerings.

The recordings may be published on the website and/or social media channel. Where feasible, State Records NSW removes images of participants and presenters displayed in the recordings.

State Records NSW will respect the wishes of those who do not wish to be included in the online recordings.

The recording is temporarily stored on a computer network while being edited or processed. The edited recording is stored electronically in the social media channel. Access to the recordings may be provided for the public or only for NSW public sector or event participants.

Conferences and other events

State Records NSW participates in external events including conferences and seminars. State Records NSW take the PPIP Act and the HRIP Act into consideration when attending events and aims to inform people how State Records NSW will manage their personal or health information if it is collected.

During these events, State Records NSW may collect general information such as the number of participants, questions participants asked, what resources were provided and general demographic information such as location of the public office.

The information collected is stored electronically on a share drive, in paper form or with an online application or tool.

Website publishing, photography, filming, and media

State Records NSW owns and maintains the website: <https://staterecords.nsw.gov.au>. This website is used to promote the State Records Act and to publish resources to help NSW public offices and other stakeholders understand the Act.

State Records NSW does not publish personal or health information on the website without permission.

Website data is stored on secure servers at external hosting providers – Acquia.

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

State Records NSW offer webinars for the public and internally to staff. If a webinar is to be recorded, the convenor will inform the participants when recording commences and ends, and where the webinar will be made available.

State Records NSW stores photos and footage electronically on its computer network along with clear instructions on the approved use of the images or footage.

4. How information is managed by State Records NSW

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

4.1 Use of personal information

State Records NSW uses the information it collects to:

- promote awareness and understanding of State Records Act to NSW public offices and NSW community
- conduct monitoring exercise within the NSW public sector
- advise staff and stakeholders on recurring trends and issues
- conduct or review complaints
- refer a complaint to a relevant authority.

State Records NSW makes sure personal information is accurate before using it. For example, State Records staff member will check contact details directly with the relevant person and may ask people to spell their names where necessary.

Personal information of State Records NSW staff is used by management, or via relevant reporting lines, specific to the staff member. The information may also be forwarded and disclosed to people management service providers supporting State Records NSW. Unless otherwise stated, the personal and health information collected by MHNSW and State Records NSW staff agency about its staff is used only for workforce management.

MHNSW also has a number of functions and obligations under the *State Records Act 1998* (SR Act).

To enable MHNSW to undertake these functions, State Records NSW may share certain types of information with MHNSW relating to Public Officers Senior Responsible Officers including:

- Name
- Title
- Organisation
- Email address
- Phone numbers

This information will be used by MHNSW workers to enable MHNSW to communicate to Public Offices regarding their obligations under the SR Act. Should SRO's not want their information shared with MHNSW

they can opt out by emailing govrec@staterecords.nsw.gov.au.

4.2 Disclosure of personal information

State Records NSW does not disclose personal information, including the ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health, or sexual activities unless it is to prevent a threat to the life or health an individual, and unless otherwise exempted under the PPIP Act, HRIP Act or SR Act.

Enquiries

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

State Records NSW does not disclose personal information about a particular enquiry to anyone outside of its office without the consent of the enquirer.

State Records NSW usually receives requests for records management contact information from NSW public offices. State Records NSW does not provide contact information without the consent of the relevant contact or person.

Complaints and reviews

State Records NSW may discuss personal information with the relevant agency when handling complaints or reviews.

State Records NSW may disclose personal information when referring complaints to the Information and Privacy Commission, the NSW Ombudsman or the Independent Commission Against Corruption.

State Records may disclose personal information to:

- the Independent Commission Against Corruption
- the Australian Crime Commission
- the New South Wales Crime Commission
- the NSW Ombudsman.
- Other agencies as required under section 73 of the State Records Act.

4.3 Storage

Information held on files at State Records NSW is kept in secure storage and the information held in the records systems, computer network or cloud applications databases is only accessible to authorised staff.

Systems and databases

MHNSW provides services for the State Records NSW in relation to:

- information and communication technologies
- finance and procurement
- human resource systems and support.

All State Records NSW electronic information is stored securely with the MHNSW computer network. MHNSW have an up-to-date Information Security Management System (ISMS) Policy that provides the security framework for managing electronic information. Under this framework:

- State Records NSW servers are backed up daily;
- State Records NSW networks are secure and require individual logins and multifactor authentication (where available);
- State Records NSW staff do not give out passwords to anyone or let anyone else use their computer login;

- the databases are made accessible to relevant network users but only modified by a restricted number of authorised users.

State Records NSW retains personal information in line with the relevant retention and disposal authorities.

Records systems and monitoring portal

Records and information received and collected is held on the State Records NSW records system, Content Manager 9 (CM9). CM9 is kept on a secure location on the computer network and access is restricted to authorised staff.

State Records NSW also manages the monitoring portal for use by NSW public offices to submit assessments of their records management programs. The monitoring portal is hosted on a cloud-based service provided by Salesforce, which is managed for State Records NSW by MHNSW. However the portal is not accessible to MHNSW staff.

Human resources system

The People and Culture team of MHNSW provides the human resources function to State Records NSW. MHNSW uses the CHRIS21 human resources system for the management of State Records employee data. The personal information of State Records NSW employees stored on the system includes names, home address, phone numbers, pay details, allowances, deductions, superannuation details, bank account and tax (including TFN).

Access to employee personnel files is limited to People and Culture staff, with level of access determined by role within the team.

Staff records are retained and disposed of in accordance with the relevant retention and disposal authority. A summary record of the service of permanent staff is retained for a minimum of 75 years

Cloud-based communication tools

State Records NSW also use cloud-based communications tools such as MailChimp and Survey Monkey.

MailChimp is used for the distribution of email communications to public office contacts and members of the public, using name and email address. Staff are encouraged to regularly delete this information from MailChimp.

Survey Monkey is used for the collection of information pertaining to services provided by State Records NSW, using name and email address.

Digital Security

Users are accountable for safeguarding their username, passwords, and other secret authentication information. Users are encouraged to:

- Use good password security practices when selecting strong passwords;
- Not share passwords or other authentication information; and
- Passwords and other authentication information must not be stored where they can be accessible by others.

Physical security

Hard copy files are located at MHNSW's Kingswood facility.

Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access and such accesses are logged. State Records NSW staff have key card access to the Kingswood facility and MHNSW Mint office. Visitors cannot enter without permission. These offices are locked outside of business hours.

When not being used, hard copy files and sensitive information are securely stored.

For sensitive documents that need to be destroyed, State Records NSW use locked bins from which the documents are securely destroyed.

Disposal

Personal and/or health information may be destroyed or deleted under authorised retention and disposal authorities, notably the General Retention and Disposal Authority – Administrative Records (GA 28), when no longer required.

A secure waste destruction service is used for paper-based documents. The certificate of destruction and authorisation for destruction is retained in CM9.

Electronic documents and data may also be disposed of. This process involves ICT staff wiping or reformatting of hard drives of computers and other equipment such as photocopier/scanners before they are disposed of or returned to leasing firms. The physical destruction of obsolete hard drives, where owned by State Records NSW may also be appropriate. A secure waste destruction service may also be used for electronic storage devices.

5. Accessing or revising your information

Everyone has the right to access personal or health information State Records NSW holds about them. Individuals also have the right to amend their own personal or health information State Records NSW holds, for example, updating their contact details.

State Records NSW is required to provide you with access to the personal 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.

To access or amend your personal or health information, email State Records NSW at govrec@staterecords.nsw.gov.au

State Records NSW staff member may also contact:

- MHNSW's People and Culture to request access or amendment of their personal or health information stored in HR systems.
- MHNSW ICT support team to request access or amendment of their contact details or access to relevant systems which stores personal or health information.
- MHNSW Governance Team, at governance@mhnsw.au can:
 - Respond to enquiries about how we manage personal and health information.
 - Respond to requests for access to and amendment of personal and health information.
 - Provide guidance on broad privacy issues and compliance

6. Your review and complaints rights

If a staff member has a complaint about the conduct of State Records NSW or a member of its staff in relation to the collection, storage, use or disclosure of personal information, a written request should be sent to governance@staterecords.nsw.gov.au so that an internal review may be undertaken.

An application for an internal review can address a breach in the IPPs, HPPs, a privacy code or the improper disclosure of personal information from a public register.

Under s. 53(3) of the PPIP Act, an application for an internal review must:

- Be in writing.
- Be addressed to State Records Authority NSW.
- Specify an address in Australia to which a notice may be sent
- Be lodged with State Records NSW within six months (or such later date as State Records NSW may allow) from the time the applicant first became aware of the conduct the subject of the application.

- Comply with such other requirements as may be prescribed by the regulations to the Act.

6.1 The internal review process

Staff can request an internal review by writing to or sending the request, along with any relevant information to the State Records NSW:

Via mail: State Records NSW
Western Sydney Records Centre
161 O'Connell Street, Kingswood NSW 2747

Via email: governance@staterecords.nsw.gov.au

To help you apply for an internal review, you can use this application form from the Information and Privacy Commission.

An application for internal review will be received by an employee of State Records NSW who has responsibility of monitoring the governance mailbox. In the first instance the application will be sent to the Executive Director of State Records NSW to authorise an appropriate reviewer. The employee authorised to review will not have been substantially involved in the matter that is the subject of the application.

If the Executive Director or the submitter establishes a conflict within State Records NSW, or otherwise deems it appropriate, the application can be sent to MHNSW Governance Team to conduct the review. As State Records NSW utilises MHNSW services as part of their agreed business partnering approach, certain applications may be shared with the MHNSW Governance Team. This will be on a case-by-case basis and when deemed appropriate.

The Reviewer will:

- Acknowledge receipt of an internal review within 5 working days
- Complete an internal review within 60 calendar days
- Write to you within 14 days after completing the review and advise you of:
 - the findings of the review, including the reasons for those findings
 - action State Records NSW proposes to take
 - reasons for the proposed action (or no action)
 - your right to have the findings and proposed action be reviewed by the NSW Civil and Administrative Tribunal (NCAT).

The Reviewer may:

- Take no further action on the matter.
- Make a formal apology to the applicant.
- Take such remedial action as deemed appropriate.
- Provide undertakings that the conduct will not occur again.
- Implement administrative measures to minimise the risk of the conduct occurring again.

State Records NSW is required to:

- Notify the NSW Privacy Commissioner of an application for internal review.
- Provide reports to the NSW Privacy Commissioner on the progress of the internal review.
- Inform the NSW Privacy Commissioner of the findings of the review and of the action to be taken by State Records NSW in relation to the matter.

If requested by State Records NSW, the NSW Privacy Commissioner may undertake the internal review.

6.2 Requesting an external review

If you are unhappy with the outcome of the internal review conducted by State Records NSW 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.

6.3 Complaints to the NSW Privacy Commissioner

You have the option to complain directly to the NSW Privacy Commissioner if you believe that State Records NSW have breached your privacy. The NSW Privacy Commissioner's contact details are:

- Phone: 1800 472 679
- Email: ipcinfo@ipc.nsw.gov.au
- Web: www.ipc.nsw.gov.au
- Address: Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000
- Postal: GPO Box 7011, Sydney NSW 2001

Delegations

- Instrument of Authority relating to release of information under *Government Information (Public Access) Act 2009*

Legislation

- *Government Information (Public Access) Act 2009 (NSW)*
- *Government Sector Employment Act 2013 (NSW)*
- *Health Records and Information Privacy Act 2002*
- *Independent Commission Against Corruption Act 1988*
- *Privacy and Personal Information Protection Act 1998*
- *Protected Disclosures Act 1994*
- *State Records Act 1998*
- *Work Health and Safety Act 2011 (NSW)*

Related Policies

- NSW Government Cyber Security Policy
- MHNSW Appropriate Use of Digital Technologies Policy

- MHNSW COVID-19 Conditions of Entry Policy
- MHNSW Cyber Resilience and Information Security Policy
- MHNSW Cyber Security Incident Response Plan
- MHNSW Internal Communications Framework
- Records Management Policy
- MHSNW User Access Control Policy
- MHNSW Working with Children and Young People Policy

Other Related Documents

- State Records NSW Collecting and managing contact information from public offices guide

Definitions

Collection	(of personal information) the way in which State Records NSW/SLM 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 State Records NSW/SLM makes known to an individual or entity personal or health information not previously known to them.
Health information	means 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	means 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	means 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	means 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	means 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	means 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.

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

Staff means any person working in a casual, temporary, or permanent capacity in State Records NSW/SLM, including consultants, contractors, and volunteers.

Superseded Documents

This policy replaces:

- Nil

Revision History

Version	Date issued	Notes	By
1.0	05.04.2023	New Policy upon establishment of State Records NSW, in accordance with the Administrative Arrangements (Administrative Changes—Miscellaneous) Order published on 16 December 2022	Content – Senior Project Officer Control – Governance Approval – Executive Director
1.1	26.04.2023	Updated section 4.1 with information on sharing information with MHNSW	Content – Senior Advisor Governance Control – Governance Approval – Executive Director

Review Date

This policy will be reviewed on 05.04.2025 (2year intervals or as needed in accordance with regulatory changes)

Contact

Governance@staterecords.nsw.gov.au or governance@mhnsww.gov.au

Appendices

- **Appendix 1** – NSW's Privacy Laws
- **Appendix 2** – Authority's duty of confidentiality

Appendix 1 - NSW's Privacy Laws

This section contains a general summary of how State Records NSW must manage personal and health information under the PPIP Act and the HRIP Act. For more information, please refer directly to the relevant law or contact State Records NSW.

The Privacy and Personal Information Protection Act

What is personal information?

The PPIP Act defines personal information as:

Information or an opinion (including information or an opinion forming part of database and whether or not recorded in material form) about an individual whose identity is apparent or can be reasonably be ascertained from the information or opinion.

Personal information does not include information:

- Contained in a publicly available publication;
- About people who have been dead for more than 30 years; and
- About individuals' suitability for public sector employment.

Health information is generally excluded here as it is covered by the HRIP Act.

The PPIP Act also allows for a number of exceptions relating to law enforcement agencies.

What are the Information Protection Principles?

The PPIP Act sets out the 12 Information Protection Principles (IPPs) in sections 8-19. A brief summary of the IPPs is listed below. For a complete description please see the PPIP Act itself or 'A Guide to the Information Protection Principles' published by Privacy NSW.

Collection

- Lawful:** Only collect personal information for a lawful purpose, which is directly related to the agency's function or activities and necessary for that purpose.
- Direct:** Only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian.
- Open:** Inform the person you are collecting the information from why you are collecting it, what you will do with it and who else might see it. Tell the person how they can view and correct their personal information, if the information is required by law or voluntary, and any consequences that may apply if they decide not to provide their information.
- Relevant:** Ensure that the personal information is relevant, accurate, complete, up-to-date, and not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.

Storage

- Secure:** Store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification, or disclosure.

Access and Accuracy

- Transparent:** Explain to the person what personal information about them is being stored, why it is being used and any rights they have to access it.
- Accessible:** Allow people to access their personal information without excessive delay or expense.

viii. Correct: Allow people to update, correct or amend their personal information where necessary.

Use

- ix. Accurate: Make sure that the personal information is relevant, accurate, up to date and complete before using it.
- x. Limited: Only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.

Disclosure

- xi. Restricted: Only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.
- xii. Safeguarded: An agency cannot disclose sensitive personal information without a person's consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities, or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

Privacy Codes of Practice

Under the PRIP Act, a privacy code of practice is a statement of how an agency proposes to depart from the IPPs or the public register provisions of the PRIP Act. A privacy code of practice can substitute for compliance with the IPPs.

Public Registers

A public sector agency that keeps a public register cannot disclose personal information except for the purposes for which the register exists. The PRIP Act also introduces a right enabling people to have personal details removed or hidden from view in certain circumstances.

Offences

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

It is an offence for State Records NSW 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; and
- Hinder the Privacy Commissioner or a staff member from doing their job.

Health Records and Information Privacy Act

What is 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 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.

What are the Health Protection Principles?

These are 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. The HRIP Act sets out

the 15 Health Protection Principles (HPPs) in Schedule 1. A brief summary of the HPPs is listed below. For a complete description please see the HRIP Act itself or 'A Guide to the Health Protection Principles' published by Privacy NSW.

Collection

- i. **Lawful:** Only collect health information for a lawful purpose that is directly related to the agency or organisation's activities and necessary for that purpose.
- ii. **Relevant:** Ensure health information is relevant, accurate, up-to-date, and not excessive, and that the collection does not unreasonably intrude into the personal affairs of a person.
- iii. **Direct:** Only collect health information from the person concerned unless it is unreasonable or impracticable to do so.
- iv. **Open:** Inform a person as to why you are collecting health information, what you will do with it, and who else may see it. Tell the person how they can view and correct their health information and any consequences that will occur if they decide not to provide their information to you. If you collect health information about a person from a third party, you must still take reasonable steps to notify the person that this has occurred.

Storage

- v. **Secure:** Ensure the health information is stored securely, not kept any longer than necessary, and disposed of appropriately. Health information should be protected from unauthorised access, use or disclosure.

Access and accuracy

- vi. **Transparent:** Explain to the person what health information is being stored, the reasons it is being used and any rights they have to access it.
- vii. **Accessible:** Allow a person to access their health information without unreasonable delay or expense.
- viii. **Correct:** Allow a person to update, correct or amend their personal information where necessary.
- ix. **Accurate:** Ensure that the health information is relevant and accurate before using it.

Use

- x. **Limited:** Only use health information for the purpose for which it was collected or for a directly related purpose, which a person would expect. Otherwise, you would generally need their consent to use the health information for a secondary purpose.

Disclosure

- xi. **Limited:** Only disclose health information for the purpose for which it was collected, or for a directly related purpose that a person would expect. Otherwise, you would generally need their consent. (Note: see HPP 10).

Identifiers and anonymity

- xii. **Not identified:** Only identify people by using unique identifiers if it is reasonably necessary to carry out your functions efficiently.
- xiii. **Anonymous:** Give the person the option of receiving services from you anonymously, where this is lawful and practicable.

Transferrals and linkage

- xiv. **Controlled:** Only transfer health information outside New South Wales in accordance with HPP 14.
- xv. **Authorised:** Only use health records linkage systems if the person has provided or expressed their consent.

Offences

Offences can be found in Part 8 of the HRIP Act. It is an offence for State Records NSW/SLM to:

- Intentionally disclose or use any health information about an individual to which the employee 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; and
- By threat, intimidation, or false representation require another person to give consent or to do, without consent, an act for which consent is required.

Appendix 2 - Authority's duty of confidentiality

Section 73 of the SR Act states:

- (1) A person who acquires information in the exercise of functions under this Act must not directly or indirectly make a record of the information or divulge it to another person except in the exercise of functions under this Act.
- (2) It is not an offence under subsection (1) if, in legal proceedings, a person:
 - (a) discloses information in answer to a question that the person is compellable to answer, or
 - (b) produces a document or other thing that the person is compellable to produce.
- (3) The provisions of any other Act imposing restrictions or obligations on a person as to secrecy or disclosure of information acquired during the administration of that Act extend to apply to a person who, in the exercise of functions under this Act, gains access to that information as a result of the information having been acquired during the administration of the other Act. For that purpose, the person who gains access to the information during the administration of this Act taken to be a person engaged in the administration of the other Act.
- (4) This section does not prevent or otherwise affect:
 - (a) the giving of access to records under Part 6 (Public access to State records after 30 years), or
 - (b) the preparation and dissemination of guides and finding aids.
- (5) This section does not apply to the divulging of information to, or to the production of any document or other thing to, any of the following:
 - (a) the Independent Commission Against Corruption,
 - (b) the National Crime Authority,
 - (c) the New South Wales Crime Commission,
 - (d) the Ombudsman,
 - (e) any other person prescribed for the purposes of this section.

State Records Authority of New South Wales Sydney, Australia