POLICY

NUMBER	21/0296	VERSION	1.0
CATEGORY	Policy	SUBJECT	Corp Governance
ISSUED BY	Governance	APPROVAL DATE	21/09/2021
AUTHORISED BY	Executive	ISSUED DATE	29/09/2021
DISTRIBUTION	Internal & External	REVIEW DATE	29/09/2023

Privacy Management Plan

Purpose

The purpose of this Privacy Management Plan (PMP) is to explain how State Archives and Records Authority of NSW (SARA) and Sydney Living Museums (SLM) collects and manages personal and health information in accordance with NSW privacy laws. This includes:

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

Please refer to Appendix 1 for more information about NSW's privacy laws.

The PMP also details how these strategies and practices will be made known to staff and outlines the procedures for internal review when breaches of privacy are reported.

While this PMP focuses on personal information collected and used by SARA/SLM, SARA's role as the custodian of State Archives generated by other public sector agencies is also covered.

Background

The PPIP Act and the HRIP Act confer enforceable rights on the people of NSW in the way public sector agencies collect, store, use and disclose personal information. The PPIP Act protects personal information through 12 Information Protection Principles (IPPs), while 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 applies to the personal information and records of SARA and SLM employees, volunteers, and contractors, as well as personal information of members of the public that is held by SARA/SLM. All SARA/SLM business teams must collect, manage, and use personal and health information in accordance with this PMP.

This PMP applies to personal and health information in all forms of data capture and information collection, storage, analysis, use, communication, reporting and disclosure, including email and other correspondence, spreadsheets, and other database applications, online and paper-based forms and meeting records, images, and surveillance records.

SARA/SLM procedures outline the details of how the PMP is implemented at a local level throughout the course of business activities.

Exemption: See 2.4 Personal information in the custody of SARA.

POLICY

1. About NSW State Archives & Records Authority and Sydney Living Museums

   The State Archives and Records Authority of NSW (SARA) and Sydney Living Museums (SLM) came under the direction of a single Executive Director on 1 July 2019. Whilst maintaining two separate legal entities, services are provided under a shared model.

1.1 NSW Department of Premier and Cabinet

SARA/SLM must comply with relevant policies written by the NSW Department of Premier and Cabinet (DPC), particularly concerning human resources, finance, procurement, and information technology policies. Personal and/or health information may be shared with DPC as the overarching agency of SARA/SLM.

1.2 NSW State Archives and Records Authority (SARA)

To understand why SARA collects and holds personal information it is necessary to detail its purpose and functions. This also provides background for the roles that SARA plays as a coordinating agency of Government and as custodian of other agencies' records which may contain personal information.

1.2.1 Purpose

SARA operates under the State Records Act 1998 (the SR Act). The SR Act provides for the creation, management, and protection of the records of public offices of the State and for public access to those records. It also establishes the State Records Authority of NSW and its Board.

SARA's fundamental purpose is to ensure that the business of the NSW Government public offices is properly documented, and the resulting records are managed efficiently and effectively for as long as they are needed, and that the State Archives Collection is developed, preserved, and used.

SARA is concerned with all aspects of recordkeeping, ranging from measures to ensure that public officials create records in the course of their duties, through the management of State records in public offices, to preserving and making records of continuing value accessible as State Archives.

SARA undertakes these roles variously as:

- A coordinating agency of Government
- A provider of services to the people and Government of New South Wales, and
- The protector and preserver of the State's official Archives.

Most State records have a finite value and can be destroyed when this value has passed. However, some are preserved because they are of enduring value to the Government and/or to the community at large or to groups and individuals within it. Records of enduring value are called archives and State records transferred to SARA’s control as archives of the State are called State Archives.

1.2.2 Functions

Section 66 of the SR Act provides that SARA has the following functions:

- To develop and promote efficient and effective methods, procedures and systems for the creation, management, storage, disposal, preservation and use of State records
- To provide for the storage, preservation, management, and provision of access to any records in its possession under the Act
- To advise on and foster preservation of the archival resources of the State, whether public or private
- To document and describe State archives in their functional and administrative context
- Such other functions as are conferred or imposed on it by or under the Act or any other law

SARA 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
- Providing centralised and cost-effective storage and retrieval services for the semi-active records of public sector agencies

- Identifying those State records which should be retained as State archives and authorising the disposal of those which should not
- Documenting and 'cataloguing' State archives in their functional and administrative context
- Storing State archives in appropriate environments and ensuring that those stored elsewhere are also stored to the necessary standards
- Using 'micro-' and 'macro-preservation' techniques to preserve the State's archives
- Making State records more than 30 years old available for public access and use
- Guiding public offices in administering public access to those State records for which they are responsible
- Interpreting, prompting, and enhancing public awareness of the State Archives Collection
- Making the best use of information technology and communications to improve our services and business

1.2.3 Duty of Confidentiality

SARA' 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 SR Act recognises this and places a special duty of confidentiality on them (see Appendix 2).

1.2.4 Sydney Living Museums (SLM)

To understand why SLM collects and managed personal information it is necessary to detail its purpose and functions. These determine the personal information that SLM collects and uses.

1.2.5 Purpose

SLM (since 2013, previously the Historic Houses Trust) is a leading government agency in Australia with responsibility for conserving, managing, interpreting, and activating places and sites of local, national, and international significance. SLM operates under the Historic Houses Trust Act 1980 (the HHT Act). It also establishes the Historic Houses Trust Board.

Established in 1980, the SLM collection includes the UNESCO World Heritage listed Hyde Park Barracks, The Mint, Australia's oldest surviving government building, and the twentieth century Rose Seidler House.

The 12 museums of the SLM collection are held 'in trust' for future generations. Each has an individual plan for its conservation and management which embraces the specific qualities, significance and histories of that place and guides the approach to activities there.

1.2.6 Functions

Section 7 of the HHT Act provides that the principal objects of the Trust are:

- To control, manage, maintain, and conserve historic buildings or places, having regard to the historic, social, and architectural interest and significance of those buildings and places,
- To collect, manage, maintain, and conserve objects and materials associated with, and of significance to, those buildings and places,
- To research and interpret the significance of those buildings, places, objects, and materials, having regard to their historic, social, and architectural interest and value
- To provide educational, cultural, and professional services (including by way of research, publications, information, public programs, and activities) in respect of those buildings, places, objects, and materials that will increase public knowledge and enjoyment of, and access to, those buildings, places, objects, and materials, and promote their place in the heritage of the State

SLM performs its functions by:

- Keeping the properties and collections in SLM's care safe and bringing the past alive through programs and activities such as education, interpretation and research, exhibitions, events, festivals, publications, and venue hire
- Operating the only public library and research collection in Australia devoted to the history of architecture, gardens, and interiors

2. How SARA/SLM collect personal and health information

SARA/SLM 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 SARA/SLM collects personal and health information during its business activities.

2.1 Staff and recruitment

SARA/SLM collects personal and/or health information from its staff members as part of the recruitment process and human resources function. SARA/SLM will never ask for more personal information than is required for that purpose.

SLM administers the human resources function of both SLM and SARA, while also working with the Department of Premier and Cabinet (DPC), as the overarching cluster, and the Department of Planning, Industry and Environment (DPIE) who administer some of the human resources functions for SARA employees, such as payroll.

2.1.1 Staff

During the recruitment process and throughout employment, information (including personal and/or health information) is collected from staff members for various reasons, such as leave management, unplanned absences, workplace health and safety and to help SARA/SLM operate with transparency and integrity.

In the exercise of its functions SARA/SLM collects and manages personal and health information about its staff including but not limited to:

- medical conditions and illnesses, including fit to work checks
- next of kin and contact details
- education
- performance and development information
- secondary employment
- conflicts of interest
- financial information for payroll purposes
- employment history

Information collected by SARA/SLM is retained to the extent necessary and managed securely.

2.1.2 Recruitment

When people apply for jobs at SARA/SLM, 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 SARA/SLM. 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 SLM to be used for employment purposes, such as payroll and setting up personnel files, and the DPIE Human Resources team for SARA employee's payroll administration. The People and Culture team at SLM keeps copies of this information in secure storage areas.

2.2 Visitors and members of the public

When members of the public visit SARA/SLM sites and museums, they may be required to provide personal information. This section outlines what information is collected and for what purpose.

2.2.1 Visiting museums

When the general public visit SLM sites or events, they must purchase a ticket either in advance online or at front of house. When purchasing general admission or program tickets online, visitors are required to create an account which includes their name, address, email address and phone number. These details are stored in Tessitura, SLM's Customer Relationship Management and ticketing system. Once an account is created, visitors can log in online for subsequent ticket purchases.

When purchasing a general admission ticket at front of house, the visitor will need to provide their postcode, but this information is not appended to an individual visitor record.

When purchasing a membership or a Sydney Museum Pass either online or at front of house (ticket that allows entry to all SLM properties for one month), visitors must provide their name, email address and phone number. Members must also provide their street address. These details are stored in Tessitura as constituent data.

Online payments are processed through a third-party payment gateway. Payment details such as date, time, mode of sale and amount of the transaction are stored in Tessitura, and encrypted credit card details are stored only for the purpose of processing refunds if required.

2.2.2 Online stores and retail

Both SARA and SLM have online purchasing facilities, while SLM also has on-site retail. When purchasing an item, customers may sign up (or log in) as a member or a guest. As a member, name, email address and postal address are collected and stored in the Customer Relationship Management (CRM) databases. As a guest, the customer will need to provide their name, email address and postal address but this information is not stored.

Online payments are processed through a third-party payment gateway and payment details are not stored by SARA/SLM.

2.2.3 Reading rooms

When members of the public wish to undertake research in the SARA/SLM collections, for example at the reading room at the Western Sydney Records Centre (WSRC) or the reading room at the Caroline Simpson Library, visitors are asked to complete a reader's ticket, either online or in person, asking for their name, address, and contact number.

SARA/SLM collects this information for workplace health and safety purposes, to enable follow up if a collection item is damaged or stolen, and to monitor interest in the collection. The information collected is stored in accordance with SARA/SLM procedures.

2.2.4 Closed circuit television (CCTV)

Overt closed-circuit television (CCTV) is installed in the public areas at the Western Sydney Records Centre and the public areas of SLM's museums. The cameras are visible, and the public is notified of the use of CCTV through prominent signage. The cameras were installed in compliance with the code of practice for the Use of Overt Video Surveillance in the Workplace.

The use of CCTV protects records, exhibition material and property by providing a deterrent from potential damage and theft and by allowing on the spot policing using monitors and capturing evidence in the event of theft or damage occurring.

2.2.5 Regional Archives Centres

SARA operates seven Regional Archive Centre across NSW, where members of the public can view original State Archives. This PMP applies to personal information collected at these centres, such as applications for reading tickets.

2.3 Communications and stakeholder engagement

As SARA and SLM are separate entities, the personal information of stakeholders is retained and used separately, for example there is no cross-marketing across SARA and SLM members.

2.3.1 Corporate clients and suppliers

SARA/SLM supplies services to a wide range of NSW public offices and other organisations and purchases goods and services from many suppliers. Personal information collected for contacts in these organisations is restricted to work contact, such as position title, telephone and fax numbers and email address. This information is collected directly from the individual, from published sources or from the organisation concerned.

SARA/SLM only collects the information as part of legal obligations, for invoicing/billing and delivery.

2.3.2 Venue hire

SLM's properties are available as venue hire for corporate and private functions, such as conferences, weddings and dining. Personal information collected for contacts in these organisations and/or individuals may include name, email, phone, address, and payment details. This information is collected directly from the individual or from the organisation concerned, or from an event agency authorised to act on their behalf.

SLM only collects the information as part of legal obligations, for invoicing/billing and delivery.

2.3.3 Subscriber, mailing and contact lists

SARA/SLM keep 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 SARA/SLM will manage it. The information generally collected includes name, email address, telephone number and postal address. SARA/SLM 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:

- recipients of SARA/SLM magazine and newsletters
- corporate clients of commercial services, such as venue hire
- chief executives, corporate records managers, and other key contacts in NSW public offices
- office holders in professional bodies, research, and community groups relevant to SARA/SLM's functions and services
- donors and corporate supporters
- contacts in regional repositories, community access points and other holders of the Archives Resources Kit, and

- contacts in other archives institutions and similar organisations.

This information is stored in SARA/SLM databases, only accessible to SARA/SLM staff using a unique password.

Contact list information is collected to enable SARA/SLM to distribute news and other information connected with its functions and to correspond with relevant people and organisations.

SARA/SLM do 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 SARA/SLM to change their details. SARA/SLM does not destroy these lists; they are kept as long as they remain current.

2.3.4 Educational and cultural services

SARA/SLM administer a wide variety of programs and activities including general admission to SLM houses and museums, education programs, public programs, exhibitions, events, festivals, and publications. SLM also opens its collections to the public through its properties, library, and collections database(s). As such, SLM communicates with a variety of audiences including general visitors, program participants, members, donors, teachers, venue hire clients and other stakeholders.

The personal information collected differs for each group but may include name, address, phone number, email address, date of birth or age range, donation history, payment information, donor's relationships, tickets purchased, events attended, concession or discount card number, social media contact details, and how a person heard about an event.

The main purposes for the collection of an individual's personal information are to process sales, send tickets or products, document donations, communicate effectively with stakeholders, comply with recordkeeping and other laws and policies, and for marketing and promotional purposes. Personal information is only stored and used for purposes that an individual has consented to.

2.3.5 Collection management

SARA/SLM maintains a range of records in a variety of formats and systems in relation to the maintenance and conservation of its historical collections. Most do not routinely contain personal information.

The main repositories of information are online catalogues or databases which provide electronic access to collections, including Axiell Collections, Vernon Collection Management System, and Image Management Security System (IMSS).

SARA/SLM collect the personal information of the source of collections item (e.g., donor) including their name, contact details, associated businesses, date of birth, websites and correspondence relating to the item. This is retained on an ongoing basis but is only accessible to staff that manage the collection and not to staff merely searching the catalogue.

2.3.6 Boards and advisory committees

SARA/SLM 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.

2.3.7 Volunteers

SLM retains the personal information of its volunteers, including name, email address, phone number, address, and next of kin. This information is collected and used for the purposes of managing the volunteer program and keeping volunteers safe while on site.

2.3.8 Photography, filming, and media

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

If a client (and their photographer) provides confirmation of use of images from their event for marketing and/or promotional purposes, the people in the images may not have all given consent, however it is at the client's discretion for the selection of images they provide. This covers both corporate and private events such as weddings.

SARA/SLM 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.

SARA/SLM stores photos and footage electronically on its computer network along with clear instructions on the approved use of the images or footage.

2.3.9 Website

SARA/SLM own and maintain two websites:

- https://www.records.nsw.gov.au
- https://sydneylivingmuseums.com.au

The websites are used to promote the activities of SARA/SLM. SARA/SLM does not publish personal or health information on the website without permission.

Website data is stored on secure servers at external hosting providers (Acquia for SARA and (Pantheon) for SLM).

2.4 Personal information in the custody of SARA

As part of its function, SARA has custody of the records of other public offices. These records can be divided into two categories:

- Records transferred to SARA as State Archives
- Records stored in the Government Records Repository

Both categories may contain personal information.

2.4.1 Providing access to State records

Section 51 of the SR Act requires public offices to make access directions in relation to the records more than 30 years old for which they are responsible, including those held by SARA as State Archives, either to open or to close them to public access.

Access directions are based on the known or likely contents of a series, group, or class of records. The Attorney General has issued guidelines on Making Access Directions under Part 6 of the SR Act 1998, under s. 52(3) of the Act. The guidelines are intended to promote consistency in the making of access directions by identifying the types of information in a record series or class that may make them open or closed to public access after 30 years. They address issues such as personal information, privacy, passage of time, security, and confidentiality. Passage of time is an important issue when decisions are made to make State records available for public access. For example, personal information does not include information relating to an individual who has been dead for 30 years. The guidelines do, however, identify types of sensitive personal information that should not be released to public access about deceased individuals until a suitable passage time.

SARA ensures that records transferred to its custody as State Archives are made available to the public only in accordance with the relevant access direction. SARA monitors access directions to assist in identifying and rectifying any inconsistencies, including access directions to records containing personal information.

Access to records closed to public access is at the discretion of the responsible public office. SARA does not facilitate such access unless that access has been properly authorised, for example, under the `special access' provisions (s. 58) of the Act.

2.4.2 Records in SARA's custody

Under s. 4(4) of the Privacy and Personal Information Protection Act, information contained in records in SARA's custody is defined as `held' by the public office responsible for the records, not by SARA.

Nonetheless, SARA helps protect personal information in such records. Both categories of records noted above are held in secure environments at the Western Sydney Records Centre. Only authorised staff have access to the records.

3. How information is managed by SARA/SLM

This section describes how SARA/SLM uses, discloses, and stores personal and health information in alignment with its main types of services and functions, i.e., how SARA/SLM comply with the IPPs and HPPs.

As SARA and SLM are separate entities, the personal information of stakeholders is retained and used separately and is clearly identifiable as SARA or SLM data.

3.1 Code of Conduct

All SARA/SLM staff are bound by the DPC Code of Conduct and must undertake annual refresher training. The Code of Conduct includes the responsible handling of information.

3.2 Collection

SARA/SLM collects all personal and health information directly from the individual except in some cases when compiling information for NSW Government contacts. When not collected directly from the individual, the information is collected from publicly available sources such as the Government Directory and telephone books.

Staff providing health information are informed as to the purpose of collecting the information.

Public clients are made aware the information is being collected and why it is collected through privacy statements on the website, on paper forms, such as when making an application for a reader’s ticket, or in commercial contracts.

Clients are informed of the use of CCTV through prominent signage in the public areas at both record centres.

3.3 Storage

The information held on files at SARA/SLM is kept in secure storage and the information held in the databases is only accessible to authorised staff. The information is not used for any other purpose and is not released outside SARA/SLM.

3.3.1 Systems and databases

All SARA/SLM’s electronic information is stored securely on each agency’s internal network. The agencies have an up-to-date Information Security Management System (ISMS) Policy that provides the security framework for managing electronic information. Under this framework:

- SARA/SLM servers are backed up daily
- SARA/SLM networks are secure and require individual logins and multifactor authentication (where available)
- SARA/SLM 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. The information is kept as long as it is relevant, is updated when necessary and deleted when no longer required.

Records management and CRMs

The main repositories of personal information are the organisation's records management system, CM9, used by both SARA and SLM, and the Customer Relationship Management (CRM) databases – State Archives Management System (SAMS) for SARA, and Tessitura, Ungerboeck and Volgistics for SLM. Tessitura is SLM's museum and public programs facing CRM system, Ungerboeck is the commercial events & education bookings CRM system, which is used for invoicing, and Volgistics is for volunteer management.

CM9 is kept on a secure location on the computer network and access is restricted to authorised staff.

SAMS contains the personal information of public clients issued with readers' tickets and is kept is on a secure location on the computer network and access is restricted to authorised staff.

SLM uses Tessitura as its CRM to manage visitors, members, and donor data. Organisation access to Tessitura is part of a consortium managed by the Sydney Opera House (SOH). Users must sign a user contract, which includes privacy considerations, and that personal information is managed to a certain standard as per the contract between consortium members. Tessitura is overseen by SOH, and SLM manages access for relevant staff members, and the creation, deletion and amendments of customer and stakeholder records.

Ungerboeck holds company and individual personal information such as name, email address and postal address, for the purposes of raising contracts and invoices, for example for venue hire. Access is restricted to authorised staff. Ungerboeck is implementing a payment portal to allow customers to provide secure payment.

CCTV tapes from the cameras are stored in secure storage accessible by only authorised staff. They are held for 30 days and then reused.

Human resources system

SLM manages the human resources function for both SARA and SLM.

SLM uses the CHRIS21 human resources system for the management of SLM employee data. The personal information of SLM employees stored on the system includes names, home address, phone numbers, pay details, allowances, deductions, superannuation details, bank account and tax (including TFN).

SARA employee records and the payroll function are managed by the NSW Department of Planning, Industry and Environment (DPIE). Information from DPIE may be shared with the SLM People and Culture team as required. DPIE privacy management processes are excluded from this PMP.

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 General Disposal Authority. A summary record of the service of every permanent SLM worker is retained on a continuing basis.

Cloud-based communication tools

SARA/SLM 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 SARA/SLM, using name and email address.

3.3.2 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
- Passwords and other authentication information must not be stored where they can be accessible by others

3.3.3 Physical security

Hard copy files are located at all SARA/SLM sites.

Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access and such accesses are logged. SARA/SLM staff have key card access to the office. Visitors cannot enter without permission. SARA/SLM offices are locked outside of business hours.

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

Older hard copy files are archived in a secure storage facility in compliance with the State Records Act 1998. For sensitive documents that need to be destroyed, SARA/SLM use locked bins from which the documents are securely destroyed.

3.3.4 Disposal

Personal and/or health information may be destroyed or deleted under authorised 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 also require authorisation. 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 SARA/SLM may also be appropriate. A secure waste destruction service may also be used for electronic storage devices.

3.4 Access and accuracy

As SARA/SLM collects most personal information directly from the individual, it is reasonable to assume that the individual is aware that the information is held by SARA/SLM, and that the information is accurate at the time it is collected. SARA/SLM alerts clients of the existence of the information by publishing the PMP on its websites.

SARA/SLM encourages individuals to advise of any change in personal information they have supplied. SARA/SLM alerts the general public of their rights of access and alteration in the privacy statement online and on hard-copy forms.

3.5 Use

SARA/SLM does not use personal information for a purpose other than for the reason it was collected unless the individual concerned consents, the new purpose relates to the original purpose, to prevent death and illness or it is otherwise permitted under an exemption under the Act. The use of personal information within SARA/SLM is governed by policies and guidelines listed below.

3.6 Disclosure

SARA/SLM 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.

3.6.1 Inter-agency disclosure

The Department of Premier and Cabinet (DPC) manages Government Information (Public Access) Act 2009 (NSW) requests on behalf of SARA/SLM, during which the release of personal and/or health information may be required.

SARA/SLM may disclose personal information to investigative or law enforcement agencies, as required (as per section 73 of the SR Act).

3.7 Identifiers and anonymity (HPP only)

SARA/SLM does not identify people by their health data unless required to carry out the work function effectively, for example in a workplace health and safety response.

3.8 Transferrals and linkage (HPP only)

SARA/SLM does not need to transfer health data outside NSW or link with health records.

3.9 Public Register Provisions

SARA is responsible for the public register of access directions. The register details the title and description and location of records covered by an access direction. If an access direction closes records to public access the register also details why the records are closed and for how long. The register does not contain personal information.

SLM does not use this public register.

4. Accessing or reviewing your information, or concerns about a breach of privacy

4.1 To access or amend your personal information

To access or amend your personal and/or health information, contact SARA/SLM with your request. To ensure your request is received by the proper staff member or team managing your information, please follow these contact guidelines:

- Enquiries – email the SARA/SLM Governance team SARA-Coord@records.nsw.gov.au
- Newsletter subscriptions – use SARA/SLM website to add or remove your details
- Staff information – speak with Human Resources team member

4.2 What do I do if I believe my privacy has been breached?

If an individual has a complaint about the conduct of SARA or SLM 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 SARA/SLM 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 SARA/SLM
- specify an address in Australia to which a notice may be sent
- be lodged with SARA/SLM within six months (or such later date as SARA/SLM may allow) from the time the applicant first became aware of the conduct the subject of the application, and
- comply with such other requirements as may be prescribed by the regulations to the Act.

4.3 What does an internal review involve?

An application for internal review will be dealt with by an employee of SARA/SLM who has the authority of the Executive Director to deal with the matter. The employee will not have been substantially involved in the matter that is the subject of the application. This will normally be the Chief Information Officer (or equivalent).

The review will be completed as soon as is reasonably practicable in the circumstances and within 60 days from the day on which the application was received.

As a result of the review SARA/SLM may:

- take no further action on the matter; or
- make a formal apology to the applicant; and/or
- take such remedial action as thought appropriate; and/or
- provide undertakings that the conduct will not occur again; and/or
- implement administrative measures to ensure that the conduct will not occur again.

SARA/SLM 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 SARA/SLM in relation to the matter

If requested by SARA/SLM, the NSW Privacy Commissioner may undertake the internal review.

4.4 How will I be informed of the outcome of an internal review?

SARA/SLM will acknowledge the receipt of an application and write to an applicant within 14 days after completing the review and advise the applicant of:

- the findings of the review (and the reasons for those findings)
- action proposed to be taken (and the reasons for taking that action), and
- the right of the applicant to have the findings, and SARA/SLM's proposed action, reviewed by the NSW Civil and Administrative Tribunal (NCAT).

5. Staff Awareness

New staff are required to undertake privacy training as part of their induction to DPC, with an annual requirement to review the Code of Conduct. SARA staff are also required to sign an additional confidentiality agreement, stored in their employee record.

Staff have been notified of this PMP through staff communications. The PMP is available to staff on the SARA Intranet or the SLM Intranet.

Roles and responsibilities

- Executive Director: responsible for overseeing the PMP; ensuring that SARA/SLM complies with its obligations under the Privacy Acts; responsible for deciding whether to provide release personal information when a formal request is made by an individual under the PIPP Act or HRIP Act; making decisions regarding internal reviews if required; accepting the service of and responding to subpoenas, warrants and judicial orders.
- Members of the Executive: responsible for supporting the Executive Director in ensuring SARA/SLM complies with the PMP and its obligations under the privacy laws; making decisions regarding internal reviews if required; promoting the PMP to relevant Managers and assist with decision-making regarding the access and amendment of personal information as required.
- Head of ICT: responsible for developing and maintaining cyber and information security policies; ensuring that the provision of those policies is carried out; and notifying the Executive of issues, risks or vulnerabilities that impact information held by SARA/SLM.
- Managers and supervisors: ensuring their respective teams comply with their obligations under the Privacy Acts, including the IPPs and HPPs; promote the PMP to staff in their team.
- All Staff: All staff must comply with the IPPs and HPPs when collecting, managing, using, and disclosing personal information; workers involved in contracting must ensure contractors or service providers comply with the privacy laws, noting that liability for compliance remains with SARA/SLM.

Delegations

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

Legislation

- Freedom of Information Act 1989
- Government Information (Public Access) Act 2009 (NSW)
- Government Sector Employment Act 2013 (NSW)
- Health Records and Information Privacy Act 2002
- Historic Houses Trust Act 1980 (NSW)
- 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

- DPC Code of Conduct
- NSW Government Cyber Security Policy
- SARA Collecting and managing contact information from public offices guidelines
- SARA/SLM Appropriate Use of Digital Technologies Policy
- SARA/SLM COVID-19 Conditions of Entry Policy
- SARA/SLM Cyber Resilience and Information Security Policy
- SARA/SLM Cyber Security Incident Response Plan
- SARA/SLM Internal Communications Framework
- SARA/SLM Records Management Policy
- SARA/SLM User Access Control Policy
- SARA/SLM Working with Children and Young People Policy
- SLM Employee Records – record keeping and access

Other related documents

- None

Definitions

- Collection: (of personal information) the way in which SARA/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 SARA/SLM makes known to an individual or entity personal or health information not previously known to them.
- Health information: 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: 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: 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: 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: 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: 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: the information privacy principles and any exemptions to those principles that apply to the IPC, which is a public sector agency.
- Staff: any person working in a casual, temporary, or permanent capacity in SARA/SLM, including consultants, contractors, and volunteers.

Superseded documents

This policy replaces:

- SARA Privacy Management Plan (approved 2019)
- SLM Privacy Management Plan (approved 2014) P14/31

Revision history

Version	Date issued	Notes	By
1	29/09/2021	New policy	Manager, Governance

Review date

Reviews will be undertaken by the Governance Team at least bi-annually, and more frequently if changes in legislation, policies or other areas require the amendment of this policy. The next scheduled review is due in September 2023.

Contact

If you require additional information, please contact the Governance team at SARA-Coord@records.nsw.gov.au

Appendix 1: NSW's Privacy Laws

This section contains a general summary of how SARA/SLM 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 SARA/SLM.

1. The Privacy and Personal Information Protection Act

1.1 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
- 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.

1.2 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

I. 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.

II. 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.

III. 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.

IV. 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

V. 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

VI. 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.

VII. 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.

1.3 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.

1.4 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.

1.5 Offences

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

It is an offence for SARA/SLM 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
- Hinder the Privacy Commissioner or a staff member from doing their job

2. Health Records and Information Privacy Act

2.1 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.

2.2 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.

2.3 Offences

Offences can be found in Part 8 of the HRIP Act. It is an offence for SARA/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
- 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 Archives and Records Authority of New South Wales Sydney, Australia