SYDNEY LIVING MUSEUMS

POLICY

NUMBER	P14/31	VERSION	1.1
CATEGORY	Policy	SUBJECT	Governance
ISSUED BY	Director	APPROVAL DATE	06/08/2014
AUTHORISED BY	Trust	ISSUED DATE	07/08/2014
DISTRIBUTION	External	REVIEW DATE	06/08/2017

Privacy Management Plan

Purpose

This Privacy Management Plan (the Plan) explains to workers, stakeholders and members of the public how Historic Houses Trust of NSW, incorporating Sydney Living Museums (SLM) collects and manages personal and health information in the course of conducting its business. It also explains how the information can be accessed and amended if required.

Background

The Information Privacy Protection Principles (IPPs) in the NSW *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) provide for the protection of personal information and for the protection of the privacy of individuals generally. Under section 33 of the PPIP Act, SLM is required to have a privacy management plan.

This Plan also details the personal and health information held by SLM and explains who a person can contact with questions, how they can access and amend their information and what to do if they think SLM may have breached the PPIP Act or the HRIP Act. This plan will also be used to train SLM workers about how to deal with personal and health information to ensure compliance with the PPIP Act and the HRIP Act.

Scope

This Plan applies to the personal information and records of SLM employees, volunteers, contractors (collectively known as SLM workers) as well as personal information of members of the public that is held by SLM. All SLM business teams must collect, manage and use the personal and health information held in accordance with this Plan.

This Plan applies to personal 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.

PLAN

1. Definitions: privacy principles, personal and health information

1.1 Privacy Principles

Both the PPIP and HRIP Acts contain sets of principles which govern how to protect personal information. They set out legal obligations for the collection, storage, access and accuracy, use and disclosure of personal and health information.

Links to the full lists of principles can be found at:

- Information Protection Principles (IPPs) – Division 1 of the PPIP Act
  Health Privacy Principles (HPPs) - Schedule 1 of the HRIP Act

1.2 Personal information

Personal information is defined by the PIPP Act as:

"…information or an opinion … about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion"[1].

[1] PIPP Act, subsection 4(1)

The form or format of the information is not relevant. SLM holds personal information in all sorts of media, such as photographs and other image formats, video and film footage, voice recordings, computer-stored records including databases, as well as paper-based formats.

SLM holds personal information in the following (this list is not exhaustive):

- paper-based and electronic files on staff, contractors, volunteers, interns and work experience students (SLM workers);
- SLM's business systems, such as CHRIS21 (HR), CRM (customer relationship management), Sunsystems (finance), Vernon (collections) and FIRST (library catalogue);
- email addresses, mailing lists and other contact details;
- staff evaluation forms;
- commercial contracts;
- conflict of interests or gift and benefits declarations;
- competition forms;
- digital images; glass plate and roll film negatives;
- archival documents;
- closed circuit television footage;
- debtor records, and
- library loan records.

1.3 Health information

Health information is relevantly defined under the HRIP Act as:

> *"(a) personal information that is information or an opinion about:*
>
> *(i) the physical or mental health or a disability (at any time) of an individual; or*
>
> *(ii) an individual's express wishes about the future provision of health services to him or her; or*
>
> *(iii) a health service provided, or to be provided, to an individual;*

While SLM does not regularly collect the health information of non-employees, SLM may hold health information in the following (this list is not exhaustive):

- sick leave applications (with or without medical certificates);
- workers' compensation case records;
- injury reports,
- emails;
- management reports;
- WHS incident reports, and
- vaccination records.

1.4 What type of information about individuals is not personal

The legal definitions of personal and health information are broad, but do exclude certain information. The exceptions most relevant to SLM, is information about an individual:

- who has been dead for more than 30 years;
- contained in a publicly available publication;
  (ie information about named or identifiable people which is published in newspapers, books or the Internet, broadcast on radio or television, posted on social media such as Facebook or Twitter, or made known at a public event like an official opening of an exhibition, because it is regarded as publicly available.).
- where it is specially protected under other laws such as the *Public Interest Disclosures Act 1994* (NSW) or contained in Cabinet information or Executive Council information under the *Government Information (Public Access) Act 2009* (NSW) (GIPA);
- which refers to a person's suitability for employment as a public sector official; for example selection reports and references for appointment or promotion. For this reason applications for such information must be made under then GIPA Act. SLM treats this information with the same care as if it were protected by privacy laws.

2. How SLM manages personal and health information

2.1 Collection of information

Information must only be collected for purposes related to the functions and activities of SLM. These functions and the information collected by SLM are set out under section 6 of this Plan.

Whenever possible, SLM must collect personal information directly from the individual to whom the information relates unless:

- the individual has authorised collection of the information from someone else; or
- in the case of information relating to a person who is under the age of 16 years—the information has been provided by a parent or guardian of the person.

For example a donor may authorise SLM to collect their personal information from their spouse, or, a parent may provide their child's personal information to SLM to be added to the SLM membership program.

Collection of personal and health information must be relevant and necessary to SLM's purpose for collecting it, and must be:

- accurate;
- up-to-date;
- complete; and
- not excessive.

The collection of information must not unreasonably intrude into the personal affairs of the individual. For example, when SLM collects personal or health information, it must:

- make it explicit that personal information is being collected;
- make it clear who is collecting the information (SLM) and provide contact details;
- explain the reason the information is being collected;
- state what are the other parties to which the personal information is usually disclosed;
- make clear the basis on which the information is being sought: or if required by law, explain what that law is; or if the supply of the information is voluntary, set out any consequences of not supplying it; and
- make clear that the person supplying the information has rights of access to, and correction of, the information.

These requirements are usually satisfied by way of a privacy statement detailing the relevant points at the time individuals are asked to provide personal information. When the collection is occurring online, the person will be alerted to the online privacy statement by linked text on the relevant page at the point that their information is being collected.

When personal or health information is collected in writing, forms may already meet some of the collection requirements and only a brief privacy statement will be necessary to meet remaining the requirements. For example: with personal information collected by way of competition entries or RSVP forms on event invitations, SLM must indicate if the contact information of respondents is intended to be kept for further contact and, if so, confirm the respondents' consent to allow the agency to collect.

When SLM collects personal or health information in another way (e.g. in person or over the phone) providers of the information must be told if the information they supply about themselves is to be retained.

When it may not be obvious that personal information is being collected, notice must be given. For example:

- where surveillance cameras (CCTV) are used for security purposes, a notice must be placed in the areas covered by the cameras in compliance with both the PIPP Act and the *Workplace Surveillance Act 2005*;
- similarly, where computer or tracking surveillance is conducted in relation to the use of SLM property by SLM workers, the users must be given appropriate notice in compliance with both the PIPP Act and the *Workplace Surveillance Act 2005*.

If unsolicited personal information is received by SLM (for example, general employment applications), it must be handled, stored or disposed of in compliance with privacy laws and record disposal authorities issued under the *State Records Act 1998*.

2.2 Storage and disposal of information

2.2.1 Retention and security of information

Personal and health information, both paper-based and electronic media, must be stored securely in SLM systems and protected from unauthorised access and alteration. SLM business systems that contain the bulk of electronically stored personal information have security safeguards that restrict access to personal information to staff on a 'need to know' basis. Information can only be accessed by limited staff and system activity such as modifications to information is traceable to particular users. Audits are undertaken periodically to ensure system security.

Personal and health information must be kept only as long as it is necessary for the purposes for which it may lawfully be used and to meet recordkeeping obligations under the *State Records Act 1998.* When it is no longer needed for business purposes, it must be destroyed as set out under 2.2.2.

SLM's use of cloud computing means that personal and health information may be transmitted to and stored by third party contractors. SLM will ensure that contractual arrangements with a cloud service provider explicitly address privacy issues to require that the provider simply holds the data and acts according to SLM instructions. SLM will also require that the provider takes such security safeguards as are reasonable in the circumstances to prevent unauthorised access or use. SLM officers responsible for approving contractual terms with cloud service providers should consider whether it is appropriate to include any of the privacy clauses set out in part 8.2 of the NSW Government Cloud Services Policy and Guidelines.

2.2.2 Authorising disposal

Personal and health information in SLM records can only be disposed of by Compliance & Knowledge staff in accordance with SLM Recordkeeping Policy, SLM's Procedure on Records Destruction and the *State Records Act 1998* (NSW).

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

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 SLM may also be appropriate. A secure waste destruction service may also be used for electronic storage devices.

2.3 Access to personal and health information

The privacy laws give individuals a right of access to information about themselves. Individuals are entitled to know whether information about them is held by SLM, the nature of the information, the main purposes for which it is used, and how they may gain access to it, including a right of correction if details are not correct. These rights do not extend to a right to know the personal information about any other individual (third party).

SLM encourages individuals to apply for access to information about themselves under the relevant privacy laws. SLM employees or former employees should follow the SLM Procedure: *Employee Records: Recordkeeping and Access*.

2.3.1 Informal access

Individuals who would like to access their personal or health information held by SLM are encouraged to contact the SLM staff member or team managing their information. For example, customers, members or news subscribers can contact general inquiries: volunteers and interns should contact the Audience Development Officer Volunteers & Interns; donors, sponsors or persons involved with the Foundation should contact the Fundraising & Development team. The relevant staff member will then advise the individual what personal or health information SLM holds in relation to the activities for which they have responsibility. SLM Members may also update much of their personal information through the Member Portal on the SLM website.

A person does not need to put an informal request in writing. If necessary, SLM may ask them to verify their identity or make a formal application instead.

If the person wants more detailed information or physical access to the personal information held, they should make a formal request under the PPIP Act or GIPA Act (see below).

2.3.2 Employee access to their personal or health information

Employees have access to their routine records of personnel administration through Kiosk. In addition, SLM provides employees and former employees a general right of access to their personnel records and certain other records containing their personal or health information.

The SLM Procedure *Employee Records: Recordkeeping & Access* provides further information on the procedures to gain access, and any restrictions that may apply. For example employees who seek access to their referees' reports are required to make a formal request under the GIPA Act.

If an employee or former employee is not granted or not satisfied with the level of informal access they have been given to their personal information, SLM encourages them to make a formal application under the PIPP Act (see 2.3.3).

2.3.3 Applying for access under the PPIP Act

Individuals who want access to more detailed personal information, or who want physical access, should make a formal request under the PPIP Act. This option is not available for employees or former employees seeking access to information about their employment or promotion, who must apply under the GIPA Act.

Requests must be made in writing using the *Form – Application to Personal Information under the PPIP Act*.There is no application fee. SLM endeavours to process applications made under the PPIP or GIPA Acts (below) within 20 working days

2.3.4 Applying for access under the GIPA Act

The GIPA Act provides a more formal process that requires payment of an application fee of $30. The request must be in writing and addressed to the SLM contact officer set out in section 5.1. The request must include:

- details of the information the applicant wants to access
- state that the request is made under the GIPA Act
- a postal address, and
- a bank or personal cheque for $30 as payment for the application fee.

Where requests are complex and/or require the commitment of significant resources to make the information available, a processing fee of $30 per hour may apply. In these cases applicants will be advised, and must agree to meet, the additional costs before SLM proceeds with the application.

The Information and Privacy Commission (IPC) website provides a range of resources for individuals wanting to access government information at the link below:

http://www.ipc.nsw.gov.au/how-do-i-get-my-information

2.3.5 Refusal of access

In some circumstances it may be appropriate and lawful for SLM to deny access, including if:

- SLM reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- providing access would have an unreasonable impact on the privacy of another individual;
- the request is frivolous or vexatious;
- the information is covered by client legal privilege
- providing access would be unlawful or if denying access is required or authorised under Australian law or a court/tribunal order; or
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

If SLM decides not to provide access, reasons will be provided to the applicant, along with details of the right to seek an internal review of the decision (see section 3.1).

2.4 Accuracy

SLM must not use personal or health information without taking reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete and not misleading. One of the reasons for the right of access to information about themselves under privacy laws is so that individuals have the opportunity to ensure the information is correct.

2.4.1 Contact information and communication

Ensuring contact information is up-to-date and accurate is an obligation under the legislation to guard against accidental disclosure of personal or health information by sending a communication to the wrong person. Particular care must be taken when using electronic forms of communication, for example, when sending email to multiple recipients, that the personal information of the other recipients is not disclosed to any individual recipient. An email address may name, or otherwise identify, the recipient and so is classified as personal information.

Use of social media such as Facebook or Twitter is limited to providing information to members of the public on a broadcast basis for approved marketing or engagement purposes. Social media must not be used for responding to any member of the public's question where the response would include personal information.

2.4.2 Verification and correction by individual

SLM workers can correct or update their 'routine' personal information by using Kiosk. Changes or corrections to names must be submitted by the individual supported by the original, relevant documents (e.g., marriage or birth certificate, passport). The original documents must be sighted by the Human Resources (HR) staff member making the amendment and then returned to the individual. This may also be done electronically (that is, by email) with scanned supporting documents. However, SLM may request the originals be presented for verification when the individual is able to visit SLM in person.

Applications for changes to non-routine personal or health information may need to be submitted to the Head of HR. This could include records or statements about a person's health, competence, or qualifications which are considered inaccurate or misleading.

The right to correct information which relates to suitability for public employment (excluded from the definition of personal information) is limited to matters of fact. The right to correct does not apply to opinions. However, the individual has the right to have placed on the record his or her response to such an opinion. The person to whom the inaccurate information relates is also entitled, providing it is practicable, to have any recipients of the inaccurate or misleading information notified of an amendment made by SLM.

Members of the public and other persons also have the right to amend their personal or health information we hold, for example if they need to update their contact details. A person may amend or correct their personal or health information by the same processes as detailed for access set out in 2.3 above.

2.4.3 Verification and correction by SLM

SLM must be satisfied of the individual's identity and authority to request the change and may request evidence of identity or authority as confirmation. SLM will consider the request and may either agree, or decline to amend the information. If SLM agrees with the request they will inform the individual once the amendment has been completed. If SLM decides not to amend the information, it must provide the reasons for the decision to the applicant as well as details of the applicant's right to seek an internal review of the decision.

All requests for amendment, decisions and correspondence in relation to requests will be attached to the relevant file.

2.5 Appropriate Use

SLM must only use personal information for the purpose for which it was collected, or for a directly related purpose, unless consent has been obtained from the individual. The use described in the privacy statement provided on all forms and in online collection of information sets the parameters for SLM's use of personal information.

Generally, only SLM workers who need access to personal information in order to carry out their duties have access to it. The personal information will be used by SLM for the purpose(s) notified at the time of collection or a directly related purpose. It must not be used for any other purposes

without authorisation from the individual.
For example, personal information may be used by another section or disclosed outside SLM in the following instances:

- where the use is directly related to the purpose for which the information was collected (e.g. a customer's email address collected for the purpose of sending event e-tickets is used to send that person updated information about that event);
- if it is necessary to prevent or lessen a serious and imminent threat to life or health of any person (e.g. providing health information if a SLM worker is taken ill);
- if it is required for investigation relating to law enforcement purposes or to protect the public revenues (e.g. criminal investigations, see 5.6 below); or
- where the use and/or disclosure is permitted by a Public Interest Direction made by the NSW Privacy Commissioner (for example the Direction on Information Transfers between Public Sector Agencies.

Photographs and images taken of individuals are also personal information and can only be used for purposes for which the subject has provided permission as documented by the release form. The form must be stored and linked to the image. Images should be deleted or otherwise destroyed in line with record disposal authorities when they are no longer in use.

2.6 Disclosure

Disclosure generally means providing an individual's personal information to another person or external organisation. SLM does not disclose personal information it holds about a past, present or prospective SLM worker, any stakeholder or a member of the public to an external third party or organisation without the individual's express consent unless required or authorised by law.

2.6.1 Express consent:

Express consent means that SLM has been in contact with the individual concerned and obtained consent to disclose information that is precise as to the kind and, if possible, the exact contents of the information to which the consent relates, and precise as to whom the information may be disclosed. An individual cannot give express consent in advance to disclosure of information which does not exist, or is unknown, at the time consent is sought. Express consent is not needed if the individual was told at the time of collection that it would be disclosed to named third parties. References for SLM workers should not be provided unless the individual has made a request for a reference, or in other words, given consent to the disclosure of the personal information.

2.6.2 Use of social media:

Social media, especially Facebook and Twitter, are increasingly used as a means of communicating with present and potential customers. Social media are considered to be communication in the public domain. Care must be taken when using social media *not* to collect or disclose any personal information. Any such communication is a SLM record and must comply with the privacy laws.

2.6.3 Exceptions to the non-disclosure rule:

In the following circumstances, disclosure of a person's personal information is allowed:

- disclosure of the personal information is required for a purpose directly related to the purpose for which the information was collected and SLM has no reason to believe the individual would object to the disclosure;
- it is reasonable to assume the individual is aware that the information is usually disclosed to the other organisation or party (this disclosure is usually included in the privacy statement the individual saw when supplying the information);
- it is reasonable to believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of the individual or any other person;
- it is required for law enforcement or investigation purposes. In such instances, a valid warrant or court order (subpoena) may be required;
- the disclosure is required, permitted, implied or reasonably contemplated by an act or any other law; and
- the disclosure is permitted by a Public Interest Direction made by the NSW Privacy Commissioner.

2.6.4 Requests from law enforcement agencies

If a SLM worker is asked by a law enforcement officer for information or documents about any person, whether in person or in writing, the SLM worker must refer the law enforcement officer to the Head of Compliance & Knowledge who will brief the relevant Member of Executive to assist with the decision regarding the release of the information.

Under no circumstances should a SLM worker provide personal information in response to a request by telephone to a party outside SLM without either the express consent of the individual to whom the information relates, or authorisation from the appropriate person (see below).

In emergency circumstances, there may be occasions when personal information is disclosed without reference to the individual for authorisation. Decisions to disclose personal information held by SLM without the consent of the individual concerned are made as follows:

- relating to SLM workers – by the Head of Human Resources;
- relating to members of the public – by the Director.

The decision maker must ensure a record of the decision is kept on file in accordance with SLM's recordkeeping policy.
SLM has the discretion to disclose personal information to law enforcement agencies without the consent of the individuals concerned or a warrant when the disclosure:

- concerns proceedings for an offence or for law enforcement purposes;
- is related to the whereabouts of a person reported as missing to the police, and the disclosure is to be made directly to a law enforcement agency;
- is reasonably necessary for the protection of public revenue or to investigate an offence where there are reasonable grounds to believe that an offence has been committed.

It is important to note that SLM is not required to disclose personal information in the absence of a search warrant, subpoena or other lawful requirement.

Subpoenas and warrants: Subpoenas or warrants, issued by a court or a magistrate, which demand the release of information or records are forwarded to the Director who will supervise the response to the subpoena or warrant. Only the Director should accept service of the documents.

Solicitors or insurance companies seeking personal information from SLM are informed that SLM will not supply personal information without the written consent of the subject of the information or a subpoena or similar court order.

2.6.5 Restricted personal information:

Some categories of personal information are given stricter protection under section 19 of the PPIP Act, including that relating to:

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

These categories of information are not generally collected by SLM, however if for any lawful purpose it is collected it may only be disclosed if:

- it is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or of another person, or
- if another act requires the disclosure.

2.6.6 Commonwealth government departments:

Various Commonwealth government departments under their legislation require SLM to disclose personal information to them. Departments with responsibilities such as social security and services (including Centrelink), immigration and taxation have a lawful need and right to access some personal information held by SLM.

2.6.7 Tax file numbers

The collection, use and disclosure of Tax File Numbers (TFN) by SLM is controlled by the *Commonwealth Privacy Act 1988*. The Commonwealth Privacy Commissioner has issued extensive, legally binding Tax file number guidelines which are available at: http://www.comlaw.gov.au/Details/F2011L02748

SLM must ensure that Tax file numbers are protected against loss, unauthorised access, use, modification, disclosure or other misuse.

2.6.8 External contractors

SLM contractors or service providers are subject to the NSW privacy laws. For the purposes of the privacy legislation, they are regarded as part of SLM and SLM is responsible if there is a privacy breach. Contractors/service providers must be made aware that personal information held by SLM to which they have access must be handled in compliance with the privacy legislation.

The contract under which they are engaged must specify what personal information is to be provided to them and include a confidentiality agreement. The contract must specify that either the personal information is returned to SLM, or destroyed in a secure manner, when the service has been completed. The contract must specify how the information is to be returned or destroyed and the service provider must certify that no copies of the information have been retained by them.

Information technology vendors and service providers who may require access to SLM's business systems in order to fulfil the requirements of their contract must sign non-disclosure agreements before they are granted access to the systems.

Contractors and non-staff SLM workers like volunteers, interns and work experience students, while working for SLM, must comply with the privacy laws just as if they were a part of SLM – as SLM is liable for any breaches. Contracts or agreements about working arrangements must include reference to privacy requirements if access to personal or health information is involved.

2.7 Use and disclosure of health information

The PPIP and HRIP Acts have different requirements relating to the use and disclosure of personal and health information. The strict rules for disclosure apply to use of health information within SLM.

SLM does not use or disclose an individual's health information for any purpose other than the original purpose for which it was collected. SLM generally collects health information directly from the individual for the purpose of complying with legal obligations as an employer and to fulfil other duties to SLM workers.

In certain circumstances, generally related to the medical purpose for which health information is originally collected, stored, provided or used, health information may be disclosed lawfully without authorisation by the individual concerned. Any purpose for which it may be lawful to disclose health information without further authorisation is referred to as a secondary purpose.

Health information must be protected from unauthorised use and disclosure wherever it is held and all authorised use and disclosure made of it should be tracked or recorded.

Health information must not be used or disclosed unless:

- SLM has obtained consent from the person;
- the information is used for a related health treatment or secondary purpose that is within the reasonable expectations of the person;
- there is a serious threat to the health, safety or welfare of the person or to public health or safety;
- it is reasonably necessary for the management of health services;
- it is necessary to find a missing person;
- there is a suspected unlawful activity or breach of Code of Conduct: Staff and Volunteers;
- it is for law enforcement purposes;
- it is lawfully authorised or required, or permitted under another law; or
- it is disclosed on compassionate grounds.

Under the NSW *Work Health and Safety Act 2011*, there is a duty to disclose information to supervisors which will reduce, eliminate or minimise risks to health or safety in the workplace.

When health information is provided by a SLM worker to a supervisor for this purpose, it should not be further disclosed except where necessary to reduce or eliminate risks. The supervisor may seek the consent of the SLM worker before further disclosing the information.

3. Complaints or requests for review of a decision

3.1 Internal review

A breach of an individual's privacy is defined as a breach of one or more of the IPPs or HPPs. An individual who considers his or her privacy has been breached can make a complaint to SLM under s.53 of PPIP Act and request a formal, internal review of SLM's conduct in relation to the privacy matter.

Applications for internal review must:

- be in writing;
- be addressed to the Privacy Officer;
- include a return address in Australia; and
- be lodged with SLM within six months of the time the applicant first became aware of the conduct which is the subject of the application.

The internal review will be conducted by an SLM worker who has not had any involvement in the matter which gave rise to the complaint of breach of privacy.

The PPIP Act requires that the NSW Privacy Commissioner be informed of the receipt of an application for an internal review of conduct, and receive regular progress reports of the investigation. In addition, the Commissioner is entitled to make submissions to SLM in relation to the application for internal review. The person processing the internal review must consider any relevant material submitted by the applicant, and the Privacy Commissioner.

SLM follows the Protocol for Handling Privacy Complaints process provided by the Office of the Privacy Commissioner.

An internal review must be completed within 60 days of the receipt of the application. The applicant is advised of the finding within 14 days of the completion of the review. As an outcome to the review, SLM may:

- take no further action on the matter;
- make a formal apology to the applicant;
- take appropriate remedial action, which may include the payment of monetary compensation to the applicant;
- undertake that the conduct will not occur again; and/or
- implement administrative measures to ensure that the conduct will not occur again.

A summary of the findings of the review must be given to the NSW Privacy Commissioner within 14 days of its completion.

3.2 External review

An individual who considers his or her privacy has been breached can also make a complaint to the Privacy Commissioner under s.45 with or without going through the internal review process of SLM.

If the applicant is unhappy with the outcome of SLM's internal review, or if SLM has not completed the internal review within 60 days, the applicant can apply to the NSW Civil and Administrative Decisions Tribunal (NCAT) to review the decision. An application to NCAT following an internal review must be made within 28 days of being notified by SLM of the result.

NCAT can review the conduct from which the complaint arose, and whether or not SLM complied with its privacy obligations. NCAT may order SLM to change its practices, apologise, or take steps to remedy any damage suffered, including payment of monetary compensation for any financial loss, or psychological or physical harm suffered by the applicant because of SLM's conduct.

For more information about seeking an external review including current forms and fees, please contact the Tribunal:

website: http://www.ncat.nsw.gov.au/ncat/index.html

phone: 1300 006228 or 1300 00NCAT

post: Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

The ADT cannot give legal advice, however the ADT website has general information about the process it follows and legal representation.

4. Communication

Following approval, the Director will alert all staff to the Privacy Management Plan by email. Electronic access is provided through the Privacy page on SLM's intranet under the policies & procedures page as well as through the SLM website at: http://sydneylivingmuseums.com.au/privacy

Reference is also made to compliance with the privacy legislation in the Code of Conduct: Staff and Volunteers which is provided to all new staff.

Any SLM worker who has a query about personal information and privacy protection may phone or email the Head of Compliance & Knowledge who acts as the Privacy Officer, or the Policy & Compliance Officer for information about compliance with the privacy legislation.

5. Contact information

5.1 Internal contact

Privacy Officer

The Mint 10 Macquarie Street, Sydney, NSW, 2000

Telephone: (02) 8239 2272

Email: privacy@sydneylivingmuseums.com.au

5.2 External contact

NSW Privacy Commissioner

Website: http://www.ipc.nsw.gov.au/contact-us-0

Post: GPO Box 7011, Sydney NSW 2001

Address: Level 11, 1 Castlereagh Street, Sydney

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

6. What information is collection by SLM and how does it relate to its functions?

SLM collects and receives many different kinds of personal information in the course of fulfilling its objects that are set out in the *Historic Houses Trust Act 1980* (NSW).

6.1 Control, management, maintenance and conservation of historic buildings

SLM maintains a range of records in a variety of formats and systems relating to the maintenance and conservation of SLM properties. Records that contain personal information include those relating to:

- Staff tenancy leases: From time to time for reasons relating to SLM's execution of this function SLM staff assume tenancy of SLM property under special agreements. The associated lease or agreements as well as related written correspondence may contain the personal information of that staff member such as their name, contact details and rent.
- Contractors: SLM contracts a number of services to external parties, including utilities, building services, and consultants. Due to the specialist nature of the heritage work, the associated contracts or agreements for sole-traders, as well as related written correspondence may contain the personal information of individual contractors. This is only personal information if they are not operating as a business, where the information is publicly available elsewhere.
- CCTV: CCTV systems are installed at a number of SLM properties as a security measure. One of the main purposes of the CCTV is to control, manage, maintain and conserve historic buildings. The CCTV systems collect personal information in the form of live footage and recordings of visiting members of the public as well as SLM workers. The monitoring, access, storage, quality and security of the CCTV systems varies at each property. SLM is currently reviewing its use of CCTV in order to ensure compliance with the PIPP Act.

- Endangered Houses Fund: This is an initiative whereby SLM acquires significant heritage properties that are at risk of demolition or unsympathetic development, and restores the properties and offers them for purchase or lease. Records (both hardcopy and electronic) relating to the transactions will sometimes contain personal information of third parties such as names, contact details and information relating to the property. This may include for example executed deeds or leases as well as the records relating to a transaction such as written correspondence between SLM and the other party/parties.

6.2 Maintenance and conservation of associated objects and materials

SLM house museums contain collections including furniture and furnishings, pictures, ceramics, glassware, silverware, household goods, family papers, photographs and personal items. Other physical collections include an archaeological collection, NSW Police plate glass negatives and a specialised collection of trade literature, pattern books and domestic furnishings focused on the history of house and garden design and domestic interiors.

SLM maintains a range of records in a variety of formats and systems (primarily hardcopy and electronic files) in relation to the maintenance and conservation of these collections. Most do not routinely contain personal information. The main repositories of personal information are online catalogues or databases which provide electronic access to collections, including:

6.2.1 Vernon CMS

Vernon is an electronic collections management system containing a catalogue of all SLM collections items and research/interpretational information related to those objects. SLM collects the personal information of the source of collections items (e.g. donor) including their name, contact details, associated businesses, DOB, websites and correspondence with SLM relating to the item. This is retained on an ongoing basis but is only accessible to staff that manage Vernon and not to staff merely searching the catalogue.

6.2.2 First LMS

FIRST is a database used to manage SLM's Caroline Simpson Library, a reference library devoted to architecture, gardens and interiors. The name, contact details, history of borrowing or reference queries of SLM workers or members of the public is collected from those persons for the purpose of managing the library collection. Access to that information is via a protected IP address and is restricted to certain library staff.

6.2.3 Image Management Security System (IMSS)

IMSS is SLM's digital asset management system. This includes digital images documenting SLM events and activities as well as archival collections images. While archive images generally do not contain personal information (for the reasons outlined at 1.4), some images of identifiable persons may contain personal information.

The main groups of images that contain personal information are portrait photographs of staff (for use on the intranet) and photographs of staff and members of the public taken as records of SLM events (e.g. Education Programs photography). SLM photographers ensure that subjects consent to be photographed and to any uses of the image. Images will not be used for any purpose (e.g. marketing) for which SLM does not have the individual's written consent. This is generally obtained at the time the photo is taken by a standard release form. SLM also collects and retains the name and contact details of the subjects of images. Images are stored in IMSS with information about approved usage. All staff have read-only access to images but only Collections and Access staff that manage IMSS can create or edit records. Similarly, access and editing rights to research/interpretational information is restricted to staff who require it for business purposes.

6.2.4 NSW Police Forensic Photography Archive (Police Collection)

SLM is responsible for the management and conservation of the Police Collection, which consists of negatives of images taken from crime scenes between 1910 and 1964. Many of these images are highly sensitive and confidential. Generally the Archive does not contain personal information as the images largely depict individuals that have been dead for more than 30 years, and the interpretational documentation is largely sourced from research of historical public information (e.g. newspaper negatives). Access and use of Archive images is restricted. See the SLM Forensic Photography Archive Policy for further information (under development).

6.3 Research & interpretation

SLM staff routinely conduct research into SLM property, collections and other things of cultural significance for the people of NSW and the nation. Records related to research and interpretation are maintained in a variety of systems (including TRIM [hardcopy and electronic], Vernon, FIRST, and IMSS) and formats (i.e. outlook, word, excel documents). While most information about individuals and data accumulated through these activities is in the public domain, from time to time there is some information which is not public and which is protected by PPIP Act. For example this may include the names, telephone, address, email and other personal information contained in correspondence with SLM of:

- donors, vendors or other sources of collection items or objects used in SLM exhibitions;
- designers or persons involved in the creation or evolution of properties or collection items;
- academics, historians or other professionals that are for example involved with research for a publication or exhibition; or
- information about individuals that is unearthed in primary research (from other than publicly available sources).

6.4 Provision of educational, cultural and professional services

SLM administers a wide variety of programs and activities including 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). The main holding of personal information is the Customer Relationship Management (CRM) system, an integrated database used mainly to manage SLM's relationships with external stakeholders including:

- Customers – individuals who purchase tickets to SLM events, programs, activities or other retail items through SLM's website.
- E-news subscribers – individuals who sign up to receive periodic email newsletters about SLM events and offers.
- Members – including individuals, families and corporate groups who become Members for benefits such as free entry to our properties, advance ticket sales to events and discounts.
- Foundation Board of Directors – are directors of the Foundation for the Historic Houses Trust of NSW which raises money to support the work of Sydney Living Museums.
- Emeritus Council – are former Foundation Directors.
- Foundation Governors – individuals who provide significant support to SLM for example by promoting the Foundation and procuring donations.
- Partners – organisations that partner with SLM in support of exhibitions or events, and
- Donors – persons or groups that have made a donation to the Foundation or SLM.

With consent, SLM collects the personal information of individuals within these groups and retains it (primarily) within the CRM on a continuing basis. Some personal information of volunteers, work experience students and interns, and HHT Trustees is also stored in the CRM. Some information from the CRM (primarily reports) are also captured in TRIM, SLM's main recordkeeping system.

The personal information collected differs for each group but may include: name; address; phone number; email; date of birth or age range; donation history; payment details; Donor's relationships; written correspondence; tickets purchased; events attended; concession or discount card number; credit card details; social media contact details; interests (related to SLM); 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 will only be stored and used for purposes that an individual has consented to. While various SLM business teams have access to the CRM, access to data is restricted on a 'need to know' basis, to ensure the information is only available to staff who need it to conduct their work.

From time to time SLM may also collect non-routine health information from members of the public, for example to follow-up an incident or health-related event on SLM premises. Information relating to an investigation is captured in TRIM, with restricted access. SLM also collects limited

health information of some customers, such as the allergies of school education or other program visitors.

6.5 Administration and support activities

SLM's principal administrative activities include: hiring/engaging and managing SLM workers, governance, managing SLM funds, procuring equipment and supplies, fundraising and managing commercial venue hire. The principal support activities include recordkeeping, information and communication technology, finance, marketing, publications and web services.

The following records are the main holdings of personal information about SLM workers and sometimes members of the public:

6.5.1 SLM workers

- SLM uses the CHRIS21 human resources (HR) system for the management of SLM employees. The personal information of SLM workers stored on the system includes: names, home address, phone numbers, pay details, allowances, deductions, superannuation details, bank account and tax (including TFN). CHRIS21 is a secure database that is only accessible only to HR staff. All activity in the system (including access and modification of data) is automatically recorded and traceable, and audits of usage and security are regularly conducted.
- Personnel files (paper-based and electronic) hold records relating to individual members of staff containing personal and health information including: names, contact details, role, salary/pay history, bank details, superannuation, tax declaration, next of kin name and contact details, self-reported health information (e.g. allergies), record of SLM flu vaccination programs, previous work history, disciplinary/misconduct records, leave record, work injury details, medical certificates, letter of offer, job application, Working with Children clearance, 100 point ID check, Criminal Record Check, immigration approvals, Centrelink correspondence, performance management records and license or permit details.
  Personnel files are kept securely in HR possession, with access strictly restricted to particular HR staff members. Staff may (conditionally) access own personnel files on request, and Managers may also access files if required for business reasons.
  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.
- Some staff records, such as those relating to grievances, misconduct or workers' compensation are held separately to personnel files. Grievance and misconduct files are held securely and privately by the Head of HR. The file will be linked to an employee's personnel file if the grievance or allegation of misconduct is upheld.
- Recruitment of staff is managed through the NSW Government's Jobs NSW website. Information about an individual's suitability for public employment is excluded from the definition of personal information and not protected by the PPIP Act. Information relating to unsuccessful applicants is retained in TRIM for 2 years to meet the minimum retention requirements for records.
- SLM requires certain staff and non-staff (for example individuals that are members of SLM tender panels) to disclose any conflicts of interest. This information is stored and retained by the relevant business team in accordance with SLM recordkeeping policy and procedures.
- Digital images are taken of some (consenting) SLM workers which are stored securely within IMSS and may be used on the SLM intranet and for other purposes.
- SLM incidentally records the personal information of SLM workers via surveillance devices (as defined in the NSW *Workplace Surveillance Act 2005*). This includes CCTV footage, computer (e.g. non-routine monitoring of SLM email and internet usage) and tracking surveillance (e.g. mobile phone devices). While surveillance data is not routinely identified to an individual, it will nevertheless contain personal information. Staff are made aware of the collection of their personal information by SLM surveillance devices by ICT policies and procedures and terms of use of devices.
- SLM maintains personal information of HHT Trustees (and members of other SLM governing bodies) in files (electronic and paper) with access restricted to senior

management and other staff members who may need to contact Trustees for SLM business. Trustees are required to annually complete a financial interest register and divulge any conflicts of interest. In addition, Trust records (such as Minutes) refer to SLM workers and members of the public from time to time.

- SLM finance records are primarily located in Sunsystems. The debtor and creditor accounts may include some personal information, for example of sole traders or of contacts with debtor/creditor organisations. Accounts data is largely de-identified. Access is password protected and strictly limited to business needs. Finance staff have full access but systems security limits which staff are able to modify creditor/debtor data. Other staff have read-only access for invoicing purposes. Activity is automatically tracked and internal and external audits are regularly conducted.
- Records related to SLM procurement may incidentally hold personal information about suppliers and vendors (for example, sole traders or property transactions).
- SLM collects personal information for marketing purposes. SLM only adds individuals to mailing or distribution lists if they provide their information for that purpose. Depending on the list, SLM may collect a person's name, postal or email address, age range, event attended and interests (relating to SLM). This is then used to send that person information about events and special offers. This information is never shared with other organisations or used for any other purposes.
  SLM may sometimes use the de-identified personal information for statistical purposes. Where an individual has provided personal information to SLM for a particular purpose (e.g. to enter a competition at a SLM event) but has indicated that they do not want to added to a mailing list, the form containing that information should be securely destroyed once the statistics have been compiled.
- The Information & Communications Technology (ICT) team manages SLM's IT infrastructure including all servers, the email system and many other business applications. Personal information is stored in the records and data held in the various systems but it is normally managed in line with the business activities outlined above. The SLM server makes an anonymous record of visits to the SLM website and retains certain information including: user's server address and top level domain name, date and time of visit to the site, pages viewed and documents downloaded by the user, sites previously visited, type of browser used and the country of origin of the user. SLM collects this information for statistical purposes only will not attempt to identify users or their browsing activities unless called upon to do so by a law enforcement agency with an active warrant.

Roles and responsibilities

- Director: responsible for overseeing the Privacy Management Plan; ensuring that 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; in accordance with the law, decides whether to disclose personal information relating to members of the public without the consent of the individual concerned; making decisions regarding internal reviews if required; accepting the service of and responding to subpoenas, warrants and judicial orders.
- Members of the Executive (Director and Assistant Directors): responsible for supporting the Director in ensuring SLM complies with the plan and its obligations under the privacy laws; making decisions regarding internal reviews if required; promoting the Plan to relevant Managers, and assist with decision-making regarding the access and amendment of personal information as required.
- Managers and supervisors: ensuring their respective teams comply with their obligations under the Privacy Acts, including the IPPs and HPPs; promote the Plan to staff in their team.
- Head of Human Resources (HR): ensuring that HR team complies with its obligations under the privacy laws, including the IPPs and HPPs, ensuring that all personnel and other staff records which hold HR personal information are securely stored with appropriate access controls; decide to provide informal access to staff and former staff to their personal information held by HR; ensuring that HR staff redact third party personal information when access is granted to an individual; ensuring the accuracy of SLM worker personal information held by HR; assisting SLM workers to correct their personal information where necessary; process formal PIPP Act

applications for SLM worker personal information held by HR in accordance with all relevant laws and policies;

- Head of Compliance & Knowledge: responsible for supervising the Privacy Officer; coordinating SLM's response to GIPA requests and overseeing SLM's response to formal PIPP Act requests; assessing requests for access/correction and recommending actions to the Director as required; making recommendations regarding SLM's response to complaints or privacy matters before NCAT, if required; managing and making recommendations regarding the updating of the Privacy Management Plan.
- Policy & Compliance Officer / Privacy Officer: responsible for acting as the main point of contact for privacy queries, requests and issues; coordinating SLM's response to formal PIPP Act requests; assessing requests for access/correction and recommending actions to the Director as required; making recommendations regarding SLM's response to complaints or privacy matters before NCAT, if required; managing and making recommendations regarding the updating of the Privacy Management Plan; providing a copy of the Privacy Management Plan to the Privacy Commissioner;
- SLM workers: All SLM workers must comply with the IPPs and HPPs in the course of their 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 SLM.

Definitions

- Child: is a person under 18 years of age, unless otherwise specified.
- Law enforcement officer: is a representative of a law enforcement agency as defined in the privacy laws, including: the Police, or the police force of another State or a Territory; the NSW Crime Commission; the Australian Federal Police; the National Crime Authority; the Director of Public Prosecutions of NSW, of another State or a Territory, or of the Commonwealth; the NSW Department of Corrective Services; and the NSW Department of Juvenile Justice.
- Personal information: has the meaning provided in section 4 of the *Privacy and Personal Information Protection Act 1998* (NSW).
- Privacy laws: means either or both of the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW).
- SLM premises: means all real property owned or operated by SLM, including under lease, license, Government agreement or otherwise.
- SLM worker: means any person engaged by SLM in a paid or unpaid capacity including: employees, contractors, volunteers, work experience students or interns.

Legislation

- *Privacy and Personal Information and Protection Act 1998 (NSW)*
- *Health Records and Information Privacy Act 2002 (NSW)*
- *Ombudsman's Act 1974 (NSW)*
- *Government Sector Employment Act 2013 (NSW)*
- *Government Sector Employment Rules 2014 (NSW)*
- *Government Information (Public Access) Act 2009 (NSW)*
- *Privacy Act 1988 (Commonwealth)*
- *Public Interest Disclosures Act 1994 (NSW)*
- *State Records Act 1988 (NSW)*
- *Work Health and Safety Act 2011 (NSW)*

Related policies

- Code of Conduct: Staff and Volunteers
- SLM Forensic Photography Archive Policy (in draft)

Other related documents

- SLM Procedure - Employee records: record keeping and access
- SLM Procedure – Records destruction procedure and related Authorisation Form
- Form – Application to Personal Information under the PPIP Act

Superseded documents

- None

Revision history

Version	Date issued	Notes	By
1	07/08/2014	Plan drafted	Policy & Compliance Officer
1.1	25/11/2014	Minor amendments in response to Privacy Commissioner suggestions.	Policy & Compliance Officer

Review date

This plan will be reviewed every 3 years. The next review date is 6 August 2017

Contact

Madeleine Bennison, Head of Compliance & Knowledge
Tel: 028239 2276
Email: Madeleineb@sydneylivingmuseums.com.au