Sydney Opera House Policy

Title:	Privacy Management Policy and Plan
Policy Number:	2026/2
Effective Date:	13 July 2026
Authorisation:	Chief Executive Officer
Authorisation Date:	30 June 2026
Superseded Policy:	2016 Privacy Management Policy and Plan
Accountable Director:	Executive Director Corporate Services and CFO
Responsible Officer:	Privacy Officer

1. CORE PROPOSITION

1.1. The Sydney Opera House (SOH) collects Personal and Health information in connection with the carrying out of its functions. The Privacy Management Policy and Plan (Policy) sets out SOH's commitment to protecting the privacy of individuals (Workers, partners, performers, customers and members of the general public) by ensuring that the Collection, storage, use and Disclosure of Personal and Health information is undertaken in accordance with the *Privacy and Personal Information Protection Act* 1998 (NSW) (PPIP Act) and the *Health Records and Information Privacy Act* 2002 (NSW) (HRIP Act).

1.2. This Policy documents key strategies and detailed activities to implement this Policy and mitigate privacy risks at SOH including:

- Providing Workers with information on how to manage Personal and Health information in accordance with the law.
- Demonstrating to members of the public how SOH meets its obligations under the HRIP Act and PPIP Act.
- Complying with section 33 of the PPIP Act which requires public sector organisations to have a privacy management plan.

1.3. SOH maintains a separate Data Breach Policy to comply with the requirements of the Mandatory Notifiable Data Breach scheme under part 6A of the PPIP Act.

2. DEFINITIONS

2.1. **Collection** – the way in which SOH acquires or gathers Personal or Health information. Collection can be by any means, including a written or online form, a verbal conversation, a voice recording or taking a picture or image.

2.2. **Disclosure** – when SOH makes known to an individual or body, Personal or Health information that the individual or body did not previously know.

2.3. **Generative artificial intelligence (AI)** – a subset of AI that generates novel content such as text, images, audio and code in response to prompts. AI technologies use large language models (LLMs) that specialise in the generation of human-like text.

2.4. **Health information**

(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 the individual, or
  (iii) a health service provided, or to be provided, to an individual, or
(b) other personal information collected to provide, or in providing, a health service, or
(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or
(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or

(e) healthcare identifiers,

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the HRIP Act generally or for the purposes of specified provisions in the HRIP Act.

2.5. **Information and Privacy Commission (IPC)** – an independent NSW Government agency with responsibilities to promote privacy rights for the people of NSW and provides information, advice, assistance and training. IPC is headed by the Information Commissioner and the Privacy Commissioner.

2.6. **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 and includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

2.7. **Sensitive personal information** – Personal information about an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.

2.8. **Workers** – has the meaning provided in the *Work Health and Safety Act 2011* (NSW) and includes all employees, and any other person engaged to undertake work in any capacity on behalf of SOH, including contractors, subcontractors and their employees.

3. SCOPE

This Policy applies to Workers when handling Personal and Health information at SOH.

4. STRATEGIES FOR IMPLEMENTING THIS POLICY

4.1. SOH's Privacy Officer will collaborate with relevant stakeholders to monitor SOH's privacy controls and provide advice regarding privacy matters when required.

4.2. SOH will communicate the Policy and relevant supporting procedures to SOH employees in a range of ways, including through SOH's intranet, printed copies, internal meetings and training. All other Workers will be made aware of the Policy.

4.3. All new SOH employees are required to complete an online module on the Code of Conduct and induction before starting with SOH. The Code of Conduct specifically refers to the importance of protecting privacy and complying with the PPIP Act and the HRIP Act and is included in the SOH annual training program. Additionally, where training on this Policy is available from time to time, all SOH employees will complete such training (and contractors will complete it where necessary).

4.4. SOH informs members of the public about SOH's privacy obligations and the public's privacy rights through the publication of this Policy on SOH's website and by providing/making available SOH's *Customer Privacy Statement*.

5. PERSONAL AND HEALTH INFORMATION HELD BY SOH

Information about Workers

5.1. SOH holds a range of Personal and Health information about Workers in a number of locations and in different formats. Examples of Personal and Health information held by SOH include:

- Personal information contained in or related to personnel records, including emergency contact details, date of birth, financial information (including bank account information and tax file numbers), educational qualifications, ethnic background, timesheets, grade and salary range.
- Health information contained in or related to personnel records, including medical certificates, fitness for duty assessments, injury management information (such as

workplace injuries incident reports, Workers compensation claims and payments and return to work plans).

- Personal and Health information, including audio recordings, images and CCTV footage and complainant details, held for the purposes of conducting workplace investigations (which must be conducted in accordance with the Camera and Access Surveillance Policy and *Workplace Surveillance Act 2005* (NSW)).
- Personal and Health information related to audit and risk work, including audit evidence collected during the performance of approved audit programs, fraud and corrupt conduct complaints and conflict of interest disclosures.

Information about others

5.2. Examples of the type of Personal and Health information held by SOH about its partners, performers, customers and members of the general public include:

- Personal and Health information related to the purchase of tickets that is collected so that SOH can deliver tickets to customers, contact them in the event of performance postponement or cancellation, or when other important information must be communicated. This information could include name and personal contact details (including telephone number, postal and email address), financial information (including credit card information), date of birth and concession numbers.
- Personal information that may be collected when customers join SOH Insiders, subscribe to SOH's mailing lists, enter competitions, participate in promotional activities, provide feedback or make a donation to SOH through any channel.
- Photographs and CCTV footage recorded while customers are on SOH premises.
- Opinions arising from general enquiries, consultation, feedback and complaints.
- Health information as a result of having provided First Aid at SOH premises.

6. HOW SOH MANAGES PERSONAL AND HEALTH INFORMATION

Information Protection Principles (IPPs) and Health Protection Principles (HPPs)

6.1. The objectives of the PPIP and HRIP Acts are to protect individuals' privacy, to allow them a degree of control over information held about them and to provide a mechanism for complaints. These objectives are achieved primarily through compliance with the 'privacy principles' (IPPs and HPPs) which establish standards for using Personal information in the NSW public sector and regulate the Collection, storage, use and Disclosure of Personal and Health information by agencies.

6.2. The most relevant obligations to SOH and how SOH ensures compliance have been condensed into one set of plain language principles in the table below. These principles should not be treated as a substitute for the principles set out in the PPIP and HRIP Acts as they do not cover their full range or complexity. Workers should always seek guidance from the Privacy Officer in relation to the application of the below principles.

COLLECTION	
Principle	**How SOH will comply**
Limiting the Collection of Personal and Health information *(PPIP Act and HPP 1*)	SOH will only collect Personal and Health information if it is: • For a lawful purpose that is directly related to SOH's functions. • Reasonably necessary for SOH to have the information for that purpose. By limiting SOH's collection of Personal and Health information to only what SOH reasonably needs, it is easier to comply with SOH's other privacy obligations. When requesting Personal or Health information on behalf of SOH, Workers should only ask for information that is reasonably necessary to the task at hand. SOH will

	especially avoid collecting Sensitive personal information if not needed. See the definition of Sensitive personal information in section 2.
Collecting Personal and Health information – the source, method and content *(9 & 11 PPIP Act and HPP 2 & 3)*	SOH will collect Personal or Health information directly from the person unless they have authorised otherwise or, in the case of Health information, it would be unreasonable or impractical to obtain the information directly from the individual. When collecting information from an individual, SOH will: • Not collect excessive Personal or Health information. • Not collect Personal or Health information that would unreasonably intrude in that individual's personal affairs. • Ensure that Personal and Health information collected is relevant, accurate, up-to-date and complete. • Have regard to the Privacy Commissioner's collection guidelines.
Notification on Collection *(10 PPIP Act and HPP 4)*	When collecting Personal or Health information from an individual (or from someone else about that individual), SOH will take reasonable steps to inform the person: • That SOH is collecting and holding the information. • Whether the collection is required by law (and if so, which law) or is voluntary. • What the information will be used for. • If any other parties routinely receive the information from SOH. • What the consequences will be for the person if they do not provide the information. • That they have a right to access and/or correct their Personal and Health information held by SOH. The name of SOH, and how to contact SOH (including the contact details of the Privacy Officer). Notification is usually provided to individuals through a 'privacy notice' at the initial time of Collection or as soon as possible. Privacy notices can be in writing or verbal. A copy of SOH's Customer Privacy Statement, which serves as notice can be found on the website, see link in 4.4.
STORAGE	
Retention and security *(12 PPIP Act and HPP 5)*	SOH will put in place reasonable security safeguards to protect Personal and Health information from loss, unauthorised access, use, modification or Disclosure, and against all other misuse. SOH will ensure Personal and Health information is stored securely, not kept longer than necessary for lawful purposes and disposed of, appropriately. Where it is necessary for SOH to transfer Personal or Health information to a third party in connection with the provision of a service to SOH, SOH will do everything reasonable within SOH's power to prevent unauthorised use and Disclosure of that information. Information security is fundamental to information privacy. SOH's information technology systems are designed to ensure that only authorised users can access them. Access controls are also employed to only give access to information required for the user's particular role and functions. Logs and audit trails will act as a deterrent against any misuse, and enable security breaches or data quality problems to be investigated. SOH will follow best practice in records management for both electronic and paper records and apply retention periods and disposal schedules in accordance with the *State Records Act 1998* (NSW). When no longer required, SOH will destroy Personal and Health information in a secure manner as appropriate. See SOH's *Records Management Policy* for more details.
Transparency	SOH will enable anyone to know, on request to SOH's Privacy Officer:

(13 PPIP Act and HPP 6)	• Whether SOH holds their Personal or Health information. • The nature of the Personal or Health information. • The main purposes for which SOH uses their Personal or Health information. • Their right to access their Personal or Health Information. The publication of this Policy promotes accountability and increases the transparency of SOH's information handling practices.
Access and alteration *(14 & 15 PPIP Act and HPP 7 & 8)*	SOH will allow people to access their Personal and Health information without excessive delay or expense. SOH will allow, and encourage, individuals to update or amend their Personal and Health information, to ensure it is accurate, relevant, up-to-date, complete and not misleading. SOH will only refuse access or a request to amend Personal or Health information where authorised by law, and SOH will provide written reasons, if requested. Where SOH amends Personal or Health information that has previously been disclosed to a third party, SOH will take reasonable steps to notify that third party of the amendment, unless it is impracticable or unlawful to do so. Where SOH refuses a request to amend Personal or Health information, SOH will, at the request of the individual concerned, attach to the information a statement setting out the amendment sought but not made. Further information about how to access and amend Personal and Health information held by SOH is provided in section 7.
USE	
Accuracy *(16 PPIP Act and HPP 9)*	Before using Personal or Health information, SOH will take reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading. SOH will ensure that information is recorded in a consistent format and attempt to confirm the accuracy of information collected from a third party or a public source where practicable. SOH will not use Personal or Health information that SOH believes is based on misleading or erroneous information. As far as possible, SOH will ensure its IT users: • Use public AI tools responsibly and ethically. IT users must not disclose or input Personal or Health information when using public AI tools and platforms. Such use or Disclosure constitutes both a data breach as defined in SOH's *Data Breach Policy* and a breach of this Policy. • Where AI-driven decisions are made, are able to explain and justify their actions and decisions. Humans must remain the final decision-maker. • Fact-check and verify all outputs before using them for any official purpose. • Do not use AI outputs that are unethical, irresponsible, biased, inaccurate or discriminative. • Will not use outputs that infringe on copyright or violate intellectual property rights. See SOH's *Acceptable Information and Technology Use and Surveillance Policy* for further information.
Purpose of use *(17 PPIP Act and HPP 10)*	SOH may use Personal and Health information for:

	• The primary purpose for which it was collected. • A directly related secondary purpose (where in the case of Health information, the individual would reasonably expect SOH to use the information for that purpose). • Another purpose permitted by law, such as where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health. • Another purpose for which the person has consented.
DISCLOSURE	
Disclosure *(18 & 19 PPIP Act and HPPs 11 & 14)*	SOH may disclose Personal information if: • The person has consented to the Disclosure. • The Disclosure is directly related to the purpose for which the information was collected, and SOH has no reason to believe that the individual concerned would object to the Disclosure. • The individual has been made aware in accordance with a privacy notice under section 10 of the PPIP Act that information of the kind in question is usually disclosed to the intended recipient. • SOH reasonably believes that the Disclosure is necessary to prevent or lessen a serious and imminent threat to life or health. SOH can generally only disclose Sensitive personal information if: • The person has consented to the Disclosure. • The Disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person. Where SOH seeks to rely on a consent-based exemption under section 26(2) of the PPIP Act to disclose sensitive personal information, Workers must consult the Privacy Officer before any such Disclosure is made. SOH may disclose Health information if: • The person has consented to the Disclosure. • The Disclosure is directly related to the purpose for which it was collected and the individual would reasonably expect us to disclose the information for that purpose. • The Disclosure is permitted by law, such as where it is reasonably necessary to prevent or lessen a serious and imminent threat to life, health or safety. SOH will not transfer Personal or Health information to a person or body who is in a jurisdiction outside New South Wales, or to a Commonwealth agency, unless the requirements of section 19(2) of the PPIP Act are satisfied being: • SOH reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles, or • the individual expressly consents to the Disclosure, or • the Disclosure is necessary for the performance of a contract between the individual and the SOH, or for the implementation of precontractual measures taken in response to the individual's request, or • the Disclosure is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the SOH and a third party, or • all of the following apply: (i) the Disclosure is for the benefit of the individual, (ii) it is impracticable to obtain the consent of the individual to that Disclosure, (iii) if it were practicable to obtain such consent, the individual would be likely to

	give it, or • the Disclosure is reasonably believed by the SOH to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person, or • the SOH has taken reasonable steps to ensure that the information that it has disclosed will not be held, used or disclosed by the recipient of the information inconsistently with the information protection principles, or • the Disclosure is permitted or required by an Act (including an Act of the Commonwealth) or any other law. When using public AI tools, SOH will comply with all legislative requirements and will not disclose or input any Personal or Health information to public AI tools.
MNDB Scheme	
Mandatory Notification of Data Breach Scheme *(Part 6A of PPIP Act)*	SOH maintains a *Data Breach Policy* that is publicly available and a supporting *Data Breach Response Plan*. SOH's Data Breach Policy defines roles and responsibilities for managing a data breach or suspected data breach in line with Part 6A of the PPIP Act.

Exemptions from compliance with the IPPs and HPPs

6.3. The PPIP Act and HRIP Act provide that SOH does not need to comply with some of the IPPs and HPPs in certain circumstances. Some examples of exemptions most relevant to SOH's functions and operations include:

- Where the receipt of Health information is unsolicited.
- Where another law permits non-compliance with certain principles.
- Where Disclosure of information is reasonably necessary for the protection of public revenue, or in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed.
- When SOH exchanges Personal information with other public sector agencies for certain purposes such as responding to correspondence from a Minister or Premier.

7. HOW TO ACCESS AND AMEND PERSONAL AND HEALTH INFORMATION

7.1. Anyone may request access to and/or alteration of their Personal or Health information by email or post. All requests should be sent to:

Post: Privacy Officer
Sydney Opera House
Bennelong Point
SYDNEY NSW 2000
Email: privacy@sydneyoperahouse.com

7.2. Requests should:

- Include the person's name and contact details (postal address, telephone number and email address if applicable).
- State whether the person is making the application under the PPIP Act or the HRIP Act.
- Explain what Personal or Health information the person wants to access or amend and the purpose of such update.

SOH will seek to respond to requests within one month of receipt.

7.3. If SOH employees want to access and/or amend their personnel file, a request may be made to SOH's Human Resources on humanresources@sydneyoperahouse.com. SOH employees may inspect their files under supervision after obtaining approval from their manager or supervisor.

8. PRIVACY COMPLAINTS AND INTERNAL REVIEWS

8.1. A person who wishes to make a complaint in relation to privacy can make any of the following:

- An informal complaint by contacting SOH's Privacy Officer.
- A formal complaint to SOH by applying for an internal review.
- A complaint to the NSW Privacy Commissioner.

How to make an informal complaint

8.2. SOH encourages individuals to try to resolve privacy concerns informally by simply contacting SOH's Privacy Officer to discuss the issue, before lodging an application for internal review.

How to make a complaint to the NSW Privacy Commissioner

8.3. Anyone can make a privacy complaint directly to the NSW Privacy Commissioner if they believe that SOH has breached an IPP or a HPP.

8.4. For more information on how the Privacy Commissioner handles privacy complaints received from members of the public, please refer to the Information & Privacy Commission's *Protocol for Handling Privacy Complaints*. Complaints directed to the Privacy Commissioner can only result in conciliated outcomes, whereas internal reviews (which are explained below) can lead to a binding determination by the NSW Civil and Administrative Tribunal (Tribunal).

8.5. The Privacy Commissioner can be contacted as follows:

Office: Information & Privacy Commission, Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000
Post: GPO Box 7011 Sydney NSW 2001
Phone: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au

How to apply for SOH's internal review

8.6. An internal review is the process by which SOH manages formal written privacy complaints. An individual who is aggrieved by SOH's conduct in relation to Personal or Health information is entitled to an internal review of that conduct by SOH.

8.7. Applications for an internal review or any written complaint about privacy received by Workers should be forwarded to SOH's Privacy Officer.

8.8. An application for internal review must:

- Be in writing, addressed to SOH and sent by email or post.
- Specify an address in Australia to which the applicant is to be notified after the completion of the review.
- Be lodged within six months from the time the applicant first became aware of the conduct that they want reviewed.

8.9. SOH may, on a case-by-case basis, accept applications for an internal review where the six month time limit has been exceeded. Reasons for lateness should be clearly set out in the written application.

8.10. An application for internal review can be made on behalf of someone else where the applicant is not able to do it themselves. E.g. the person is not literate in English or has a disability. Where there is no other organisation making the application on their behalf, Workers should help the person to write their application and use a professional interpreter, if necessary. Applications in languages other than English will be accepted and translated, and all acknowledgments and correspondence to the applicant will be translated.

Internal review process

8.11. When SOH receives an internal review application, SOH's Privacy Officer will:

- Send an acknowledgment letter to the applicant within five working days and advise that, if the internal review is not completed within 60 days, they have a right to seek a review of the conduct by the Tribunal.

- As soon as practicable, send a letter to the Privacy Commissioner with details of the application. SOH will keep the Privacy Commissioner informed of the progress of the internal review.

8.12. Internal reviews follow the process set out in the Information & Privacy Commission's *Internal Review Checklist* which is available here.

8.13. If the complaint is about an alleged breach of the IPPs or HPPs; the internal review will be conducted by SOH's Privacy Officer or by another person who:

- Was not involved in the conduct which is the subject of the complaint,
- Is an employee or an officer of SOH, and
- Is qualified to deal with the subject matter of the complaint.

8.14. When the internal review is completed, as soon as reasonably practicable and within 14 calendar days**,** SOH's Privacy Officer will notify the applicant in writing of the:

- Findings of the review and reasons for those findings,
- Action SOH proposes to take and reasons for the proposed action (or no action), and
- Applicant's entitlement to have the findings and the proposed action reviewed by the Tribunal.

SOH will also send a copy of that letter to the NSW Privacy Commissioner.

External review by the Tribunal

8.15. Anyone can seek an external review if they are not satisfied with the outcome of an SOH internal review or with SOH's action in relation to the individual's application for internal review. Individuals can also seek an external review if they do not receive an outcome of the review within 60 days.

8.16. To seek an external review, individuals must apply to the Tribunal. Generally a person must seek an internal review before they have a right to seek an external review.

8.17. The Tribunal has the power to make binding decisions, and may require SOH to (among other things):

- Refrain from any conduct or action which breaches an IPP, HPP, privacy code of practice or health privacy code of practice.
- Perform in compliance with an IPP or HPP.
- Correct information disclosed by SOH.
- Take steps to remedy loss or damage.

8.18. The Tribunal may also require SOH to pay damages of up to $40,000 if the applicant has suffered financial loss, or psychological or physical harm because of SOH's conduct.

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

Office: NSW Civil and Administrative Tribunal
Level 10, John Maddison Tower 86-90 Goulburn Street
SYDNEY NSW 2000
Phone: 1300 006 228 or 02 9377 5859 (TTY)
Website: www.ncat.nsw.gov.au

9. RESPONSIBILITIES

9.1. **Workers** are responsible for:

- Complying with this Policy and supporting procedures.

- Not intentionally using or disclosing any Personal information or Health Information about another person, to which the Worker has or had access in the exercise of their official functions (other than in connection with the lawful exercise of their functions).
- Not inputting or disclosing Personal or Health information to public AI tools or platforms.

9.2. **Managers and supervisors** are responsible for leading by example and ensuring that their teams are aware of their privacy responsibilities and comply with this Policy. They are aware that intentional misuse of Personal or Health information could lead to criminal liability.

9.3. The SOH **Privacy Officer** is responsible for:

- Providing advice to SOH employees and SOH's Executive Team on privacy issues and the application of the PPIP and HRIP Acts.
- Providing a first point of contact for members of the public for all matters related to privacy and the handling of Personal and Health information within SOH.
- With assistance from SOH's Learning and Development team, providing regular training to SOH employees on the PPIP and HRIP Acts.
- Conducting internal reviews into possible breaches of the PPIP and HRIP Acts.
- Liaising with the NSW Information and Privacy Commission and other government agencies regarding privacy matters at SOH.
- Leading and coordinating the review of this Policy and any other associated procedures on a regular cycle and immediately following any significant adverse privacy event, and otherwise as required.

9.4. **Legal Team** is responsible for supporting the Privacy Officer in managing SOH matters relating to privacy.

9.5. The **Director responsible for privacy matters** is responsible for:

- Overseeing the implementation of this Policy.

10. RELEVANT LEGISLATION

- Privacy and Personal Information Protection Act 1998 (NSW)
- Health Records and Information Privacy Act 2002 (NSW)
- Privacy and Personal Information Protection Regulation 2019 (NSW)
- Health Records and Information Privacy Regulation 2022 (NSW)
- Government Information (Public Access) Act 2009 (NSW)
- State Records Act 1998 (NSW)
- Ombudsman Act 1974 (NSW)
- Public Interest Disclosures Act 1994 (NSW)
- Surveillance Devices Act 2007 (NSW)
- Workplace Surveillance Act 2005 (NSW)
- Work Health and Safety Act 2011 (NSW)

11. SOH SUPPORTING DOCUMENTS

- Acceptable Information and Technology Use and Surveillance Policy
- Code of Conduct
- Data Breach Policy
- Information Classification Policy
- Information Security Management System (ISMS) Policy

- Records Management Policy

Version History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Chief Executive Officer	19/10/2016	16/10/2016	New policy.
1.1	Chief Executive Officer	15/05/2024	15/05/2024	Updates to refer to the appropriate use of public generative AI platforms.
2.0	Chief Executive Officer	30/06/2026	01/07/2026	Full review.

APPROVED

Chief Executive Officer

Date: 30 June 2026