

Sydney Opera House Policy

Title:	Records Management Policy
Policy Number:	2023/7
Effective Date:	12/09/2023
Authorisation:	Chief Executive Officer
Authorisation Date:	12/09/2023
Superseded Policy:	Records Management Policy SOH137
Accountable Director:	Executive Director, Corporate Services & CFO
Responsible Officer:	Information Manager

1. CORE PROPOSITION

The Records Management Policy (Policy) sets out:

- How the Sydney Opera House (SOH) meets its Records management obligations in accordance with the *State Records Act 1998 (NSW) (Act)* and other legislation, policies, standards and requirements issued by the NSW Government.
- SOH's approach to the creation, capture, control, use, maintenance and disposal of SOH Records and enables SOH to maintain a strategic, structured and consistent approach to recordkeeping in line with the Act.

2. SCOPE

2.1. This Policy applies to all:

- SOH business units and Workers.
- Aspects of SOH's operations and Records that provide evidence of work-related activities, decisions or actions.

2.2. Procedures and guidelines supporting this Policy are referred to in section 7 below.

3. DEFINITIONS

3.1. **Appraisal** – the process of evaluating business activities to determine which Records need to be captured and how long the Records need to be kept to satisfy legal obligations and meet business needs, accountability and community expectations. Appraisal decisions include Records retention, destruction or transfer to State Archives.

3.2. **Authority** – State Records Authority NSW.

3.3. **Digital recordkeeping systems** – information systems with recordkeeping functionality to ensure authenticity, reliability, integrity, useability and access to Records over time.

3.4. **Disposal authority** – instrument defining the disposition actions (i.e. retention periods) that are authorised for specified Records by the Board of State Records & Archives NSW (*ISO 15489 1*).

3.5. **High-risk and high-value records** – Records related to the core objects and functions of SOH (as set out in the *Sydney Opera House Trust Act 1961 (NSW)*). In line with guidance from the Authority, these include Records that:

- Have enduring value and significance to the organisation and broader community.
- Are created or received in high-risk areas of the business, or high-risk business processes or functions.
- Would pose a significant risk to the organisation if they were misused, released inappropriately or inappropriately accessed and altered, lost, damaged or destroyed.

- 3.6. **Record(s)** – SOH physical and digital information created, received and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in transaction of business, such as documents, emails, voicemail messages, handwritten notes, social media posts and metadata.
- 3.7. **State archive** – any State record selected for permanent retention (based on its continuing historical value) that is subject to the control of the State Records Authority NSW.
- 3.8. **State record** – any Record, made and kept, or received and kept, by any employee in the course of the exercise of official functions at SOH, for any purposes of SOH, or the use of SOH.
- 3.9. **Worker** – 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.

4. PRINCIPLES

- 4.1. SOH Records are valuable business assets and integral to good business. They form SOH's corporate memory, ensuring information is captured and used to:
 - Support strategic and daily operations.
 - Meet legal obligations and stakeholder expectations.
 - Maintain state, national and world heritage values.
- 4.2. SOH, as a 'public office', has obligations under the Act in relation to the protection and management of State records. These include obligations to:
 - Make and keep full and accurate State records of SOH's activities.
 - Establish and maintain a State records management program in accordance with standards and codes of best practice.
 - Make arrangements with the Authority for monitoring of the State records management program.
 - Report to the Authority on the implementation of the State records management program.
 - Ensure the safe custody and proper preservation of State records in SOH's control.
 - Ensure that arrangements are in place for the safekeeping, proper preservation and return of those State records in SOH's control, but in the possession or custody of another.
 - Develop plans to transfer State records required as State archives into the State Archives Collection.
- 4.3. This means that SOH must do the following in relation to its Records:
 - Routinely create and manage Records as part of normal business practice.
 - Capture and store Records in authorised systems that can manage them effectively for as long as legally required.
 - Maintain and protect Records from unauthorised or unlawful access, destruction, loss, deletion or alteration, in line with legal and business requirements.
 - Share Records and make them available and accessible to those with a business need to access and use them.
 - Preserve Records across formats and systems to ensure they remain accessible and usable for as long as required.
 - Retain and/or dispose of Records appropriately, securely and in a timely fashion, including the transfer of State archives, in line with currently approved disposal authorities and SOH guidelines.
 - Implement, monitor and review recordkeeping practices and systems to ensure accountability obligations, compliance requirements and business needs are met.

5. HIGH-RISK AND HIGH-VALUE RECORDS

- 5.1. Records and information management must be a designed component of all SOH systems and service environments where high-risk and high-value business is undertaken.

5.2. High-risk and high-value records must be:

- Identified and preserved across all SOH systems and service environments.
- Sustained through system and service transitions by strategies and processes specifically designed to support the function of the organisation and accountability.

6. THIRD-PARTY SERVICE PROVIDERS

All contractual engagements with third-party service providers (including outsourced, cloud-based and similar service arrangements) must incorporate compliance with the Policy. Agreements must take into account retention and disposal requirements for Records held in providers' systems and migration of data and Records to a Digital recordkeeping system when information systems are decommissioned.

7. SUPPORTING DOCUMENTS AND GUIDANCE

7.1. The following policies, procedures and guidelines (available via Intouch) provide more detailed information in relation to specific recordkeeping issues:

- Information Security Management System (ISMS) Policy
- Information Classification Policy
- Privacy Management Policy and Plan
- Access to Information (GIPA) Policy
- Records management procedures
- Local Business Rules (LBRs) template.

7.2. Training and ongoing guidance in the application of the Policy and supporting documents are available to all Workers, including materials available on Intouch and support from the Information Management team.

8. ROLES AND RESPONSIBILITIES

8.1. **Anyone who creates a Record for SOH** is responsible for dealing with the Record in line with this Policy and supporting documents.

8.2. The **Records Management Specialist** is responsible for:

- Developing and reviewing Records and information management procedures about all aspects of Records management.
- Incorporating electronic recordkeeping requirements into operational and maintenance plans.
- Advising the Information Manager on Records management issues, including Appraisal, disposal, preservation and access directions.
- Delivering the Records management training program and providing support and advice to Workers.
- Administering the SOH Electronic Document and Records Management System (EDRMS).
- Authorising the disposal or destruction of Records and undertaking Records management operations, including transfer, recall and disposal of Records, in line with the Delegations of Authority Manual.

8.3. The **Information Manager** is responsible for:

- Developing and implementing Records and information strategies to support this Policy.
- Identifying risks to Records and ensuring appropriate controls are implemented to manage or mitigate risks.
- Developing, implementing and regularly reviewing the Policy and supporting documents.
- Maintaining, monitoring and reviewing departmental recordkeeping systems and measuring compliance with the Policy.
- Ensuring migration of digital Records is conducted in accordance with the conditions specified in standards issued under the Act and Disposal authorities.

- Ensuring that all Records are kept and accessible for as long as required by Workers, the NSW Government and the public.
- Developing and reviewing SOH public access directions and transfer plans to the Museum of History NSW.
- Authorising the disposal or destruction of Records, in line with the SOH Delegations of Authority Manual.

8.4. **Managers and supervisors** are responsible for:

- Ensuring business units and Workers under their management are aware of their responsibility to maintain accurate Records and comply with the Policy.
- Ensuring that Workers within their teams undertake Records management training.
- Implementing measures to monitor compliance and address inadequacies in recordkeeping practices.
- Working with the Information Management team to develop and implement LBRs that align with the Policy and support and meet business area Records management needs.
- Authorising the destruction of Records, in consultation with the Information Manager.
- Ensuring Records and information management is integrated into work processes, systems and services.
- Consulting with the Information Manager when introducing new processes to ensure Records are captured and remain authentic, complete, accessible and useable.
- Arranging regular internal reviews of Records in business systems and cloud-based solutions. These audits must be conducted by the system owner in consultation with the Information Manager.
- Determining legislative requirements for Records relating to their specific activities through consultation with the Information Manager and/or Legal.

8.5. The **Chief Technology Officer** is responsible for:

- Ensuring EDRMS and other business systems are available, reliable and accessible to Workers as required and that new and existing business systems comply with this Policy.
- Authorising each approved recordkeeping system, in consultation with business managers.
- Providing support and infrastructure to ensure that digital Records are managed so that they are accessible, readable, protected, complete, comprehensive and authentic for as long as required.
- Developing disaster recovery plans for digital Records and maintaining a high-value information assets register.
- Ensuring the decommissioning of systems takes into account retention and disposal requirements for held information and data.
- Implementing information security measures, including routine and comprehensive back-ups, in line with the ISMS Policy.

8.6. The **Executive Director, Corporate Services & CFO (Senior Responsible Officer)** is responsible for:

- Ensuring this Policy is regularly reviewed and up-to-date.
- Representing Records and information management interests to the Executive team.
- Approving the strategic direction of the Policy and supporting documents and ensuring that it is appropriately resourced.
- Supporting and fostering a good recordkeeping culture.
- Ensuring SOH adheres to appropriate record retention and disposal requirements.
- Arranging external audits of systems with High-risk and high-value records as needed.
- Approving SOH public access directions and transfer plans to the Museum of History NSW.

8.7. The **Chief Executive Officer** is responsible for:

- Ensuring SOH complies with the Act and the associated standards and requirements.
- Nominating the Senior Responsible Officer to oversee the operation of the Policy and the recordkeeping compliance.

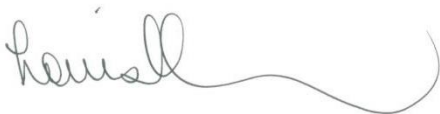
9. RELEVANT LEGISLATION AND STANDARDS

- Copyright Act 1968 (Commonwealth)
- Functional Retention and Disposal Authority: FA402 (NSW)
- General Retention and Disposal Authority: Administrative Records GA28 (NSW).
- Government Information (Public Access) Act 2009 (NSW)
- Health Records and Information Privacy Act 2002 (NSW)
- Privacy and Protection of Personal Information Act 1998 (NSW)
- State Records Act 1998 (NSW)
- Standard on records management (Standard No. 12, issued March 2015, amended October 2018)
- Standard on the physical storage of State Records (Standard No. 13, issued February 2019)

Version History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Chief Executive Officer	02/07/2019	02/07/2019	New policy.
1.1	Chief Executive Officer	12/09/2023	12/09/2023	Review to update how SOH meet its records management obligations under the relevant legislation and standards.

APPROVED



Chief Executive Officer

Date: 12/09/2023