

PRIVACY MANAGEMENT PLAN



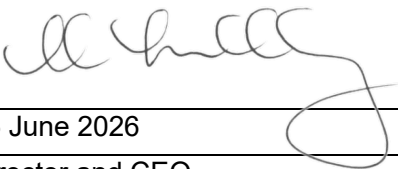
Effective Date	25 June 2026	Next Review	In 3 years
Approval	Director and CEO 		
Approval Date	25 June 2026		
Executive Policy Owner	Director and CEO		
Responsible Officer	General Counsel, Associate Director, Legal		
Version	1		
Trim No.	D26/3485		

Table of Contents

1. Introduction and Scope	4
2. Types of Personal and Health Information We Collect and Why	5
3. How We Handle Personal and Health Information	10
3.1. Lawful Collection (IPP1)	10
3.2. Direct Collection (IPP 2)	10
3.3. Notification (IPP 3) and Transparency (IPP 6).....	11
3.4. Relevance (IPP 4).....	11
3.5. Storage and Security (IPP 5)	11
3.6. Access and Accuracy (IPPs 7-9)	12
3.7. Use and Disclosure (IPPs 10-12)	12
3.8. Safeguards on Disclosure (IPP 12)	13
4. Specific Disclosure Arrangements	13
4.1. Third Party Service Providers	13
4.2. Other Government Agencies	14
4.3. Australian Museum Foundation	14
5. Health Information	15
6. Artificial Intelligence	15
7. Special Provisions, Relevant Legislation and Public Registers	16
7.1. Codes of Practice and Public Interest Directions	16
7.2. Relevant Legislation	16
7.3. Public Registers.....	16
8. Data Breach Management	16
9. Complaints and Review Processes	17
9.1. Internal Review Rights and Procedures.....	17
9.2. Informal Complaint Resolution	17
9.3. Role of the Privacy Commissioner.....	17
9.4. External Review by NCAT.....	18
10. Implementation and Compliance	18

10.1.	Privacy Officer Functions	18
10.2.	Training and Awareness	18
10.3.	Privacy Impact Assessments	19
10.4.	Public Education Initiatives	19
10.5.	Compliance Auditing	19
10.6.	Breaches and Offences	19
11.	Related Policies and Procedures	19
12.	Definitions and abbreviations	20
13.	Contact Information	21
14.	Accessibility and Review	21

Acknowledgement of Country

The Australian Museum acknowledges that we operate on the lands, waters and skies of many First Nations Peoples. As Australia's first museum, we share the responsibility of advocating for Country and honouring First Nations Peoples and knowledges.

1. Introduction and Scope

1.1. Australian Museum's Commitment to Privacy

The Australian Museum is committed to protecting the privacy of personal and health information in accordance with applicable privacy legislation. We recognise the importance of privacy in maintaining public trust and are dedicated to implementing best practices in privacy management across all our operations.

1.2 Purpose and Objective

This Privacy Management Plan has been developed in accordance with section 33 of the Privacy and Personal Information Protection Act 1998 (NSW) (**PPIP Act**) which requires all NSW public sector agencies to prepare and implement a privacy management plan.

The purpose of this Plan is to:

- establish a framework for the Australian Museum to collect, store, use, and disclose personal information in accordance with the PPIP Act and the Information Protection Principles (**IPPs**).
- demonstrate how the Australian Museum upholds and respects the privacy of its staff and individuals who deal with the Australian Museum, including our visitors, members, donors, contractors and suppliers.
- provide guidance for Australian Museum staff in dealing with personal and health information to ensure compliance with the PPIP Act and the Health Records and Information Privacy Act 2002 (NSW) Act (**HRIP Act**) (together, the Acts).

The objective of this Privacy Management Plan is to ensure that the Australian Museum manages personal information in accordance with the PPIP Act and health information in accordance with the HRIP Act.

1.3 Scope

This Privacy Management Plan applies to all employees, contractors, volunteers, and partners of the Australian Museum who handle personal and health information. It covers all personal information and health information collected, used, stored, and disclosed by the Museum in carrying out its functions.

Personal information is information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information includes information or an opinion forming part of a database, whether or not recorded in a material form (section 4 of the PPIP Act).

Health information is any personal information that is information or an opinion about a person's physical or mental health or disability or the provision of health services to them, including an individual's express wishes about the future provision of health services to them. It also includes genetic information that is or could be predictive of the health of a person or their genetic relative as well as any personal information that was collected to provide, or in providing, a health service, or in connection with donation of body parts, organs or body substances (section 6 of the HRIP Act).

Exclusions: Both the PPIP Act and HRIP Act exclude from the definition of personal and health information, information which:

- relates to a person who has been dead for more than 30 years; or
- is contained in a publicly available publication; or
- refers to a person's suitability for employment as a public sector official.

The definitions also exclude information about named or identifiable people which is published in newspapers, books or the internet, broadcast on radio or television, posted on social media.

2. Types of Personal and Health Information We Collect and Why

The Australian Museum collects and holds various types of personal information and health information to fulfill its functions as a museum and a cultural and scientific institution. The following sections outline the main categories of personal information collected or held by the Australian Museum. These categories reflect the Australian Museum's core functions, including scientific research, collection management, exhibitions, public engagement, education programs, and corporate services.

2.1. Employment-Related Information

The Australian Museum collects and holds personal information about employees, volunteers, contractors, and job applicants including:

- Personal details (name, date of birth, contact information)
- Identification documents for employment verification purposes
- Employment history and qualifications
- Performance management information
- Payroll and taxation information
- Leave and attendance records
- Workers' compensation and injury and illness management information (including workplace adjustment requests) management of non-work related injury or illness information and Independent Medical Examination records)
- Health monitoring records required or recommended under WHS Regulations
- Occupational vaccination records
- Working with Children Checks
- Background and reference check information
- Candidate relationship disclosure information
- Conflict of interest declarations and declarations of gifts and benefits received
- Digital images of staff for identification and security purposes
- Diversity information provided by staff on an optional basis.

2.2. Visitor Information

The Australian Museum collects personal information from visitors to the museum and members of the public including:

- Contact details (including name, address, email address and phone number) for mailing lists, general communications and ticketing for exhibitions and events,
- Marketing and communications preferences
- Membership and subscription details
- Visitor feedback and survey responses
- Images from security cameras and photography
- Incident reporting information
- Website usage data and cookie information.

People visiting the Museum for business purchases, such as contractor and supplier personnel, are also required to provide their personal information on entry to the Museum for safety and security purposes.

2.3. Donor and Fundraising Information

The Australian Museum collects and maintains information about donors and supporters including:

- Contact details (including name, address, email address and phone number) of people who make donations
- Donation history and preferences
- Financial information for processing donations
- Communications preferences
- Event attendance information.

2.4. Information Related to Collections

The Australian Museum holds personal information in relation to its collections including:

- Information about object donors
- Provenance information about cultural objects
- Details of lenders for exhibitions
- Information about artists and creators
- Research relating to collection items.

2.5. Scientific Research Information

The Australian Museum Research Institute (AMRI) and the Lizard Island Research Station collect personal information in connection with scientific research and related activities, including:

- Grant recipient and grant funding information, including financial information for processing receipts and payments
- Visiting researcher and fieldwork participant information, including where necessary, professional credentials and qualifications, contact details, emergency contact details, medical information and medical history and dive certifications
- Liability waivers
- Research collaborator details
- Indigenous knowledge and cultural information (in accordance with the Australian Museum's Indigenous and Cultural Intellectual Property Policy)
- Field research data that may contain personal information or identifiers
- Citizen science participant information collected in connection with citizen science projects such as FrogID
- Contact details for research fellows, volunteers and interns.

Anonymised or pseudonymised information may also be used or disclosed for scientific research and evaluation purposes.

2.6. Education and Public Programs

The Australian Museum collects personal information in connection with its education and public programs including:

- Program participant details
- School group information and staff contact details
- Presenter and facilitator information
- Feedback and evaluation data
- Volunteer contact details
- Event registration information, including financial information for processing payments.

2.7. Information Relating to First Nations People

The Australian Museum collects and holds information relating to Aboriginal and Torres Strait Islander peoples including:

- Cultural and traditional knowledge (with appropriate permissions and subject to the Australian Museum's Indigenous and Cultural Intellectual Property Policy)
- Information about cultural heritage and objects
- Community consultation records
- Repatriation records
- Details of community members engaged to consult on or participate in AM projects.

2.8. Supplier and stakeholder information

The Australian Museum collects and holds information relating to its suppliers and stakeholders. This information is collected in the ordinary course of the AM's activities, including procurement, contract management, events, research, fieldwork, exhibitions, programs and stakeholder engagement activities. The information typically includes:

- Business contact information (such as names, job titles, email addresses, and telephone numbers of individuals at supplier or partner organisations)
- Details of public officials and government agency contacts
- Information about contractors, consultants, and other individuals engaged to provide goods or services to the AM
- Information provided in the course of tender processes, expressions of interest, or supplier due diligence.

2.9. Website, Digital Applications and Social Media Interactions

The Australian Museum collects personal information through interactions with individuals via the Australian Museum website, digital applications (such as FrogID) and social media channels including:

- when individuals purchase goods or services from us, such as tickets or products from our online retail shop
- when individuals subscribe to newsletters, register for events, or enter competitions
- User profile information from followers and commenters on social media platforms
- Content shared on the Australian Museum social media platforms
- User-generated content
- Social media analytics data
- Direct messages and communications.

2.10. Health Information

The Australian Museum collects health information only where necessary for AM's functions. Health information is held primarily in connection with employment and people management functions administered by the People & Culture team, and in limited circumstances in connection with fieldwork and research activities for safety purposes. Types of health information that is collected by the Museum includes:

- Employee medical certificates or Certificate of Capacity (for workers compensation claims), independent medical examination records and return to work plans
- Health monitoring records required or recommended under WHS Regulations
- Occupational vaccination records
- Ergonomic assessments and workstation assessments

- Health information provided by job applicants, employees and volunteers requesting reasonable adjustments during the application process and to support them in their job
- Health information provided by participants in fieldwork projects and expeditions
- Diving certifications in relation to Lizard Island and other field operations
- Work health and safety incident reports
- First aid information for visitors, staff, volunteers and contractors
- Accessibility requirements for visitors and program participants
- COVID-19 and other public health-related information when required.

2.11. Financial Information

The Australian Museum collects credit card information for the purpose of processing online purchases of tickets, programs, and merchandise through our online and on site retail store. This information is transmitted using secure encryption protocols and processed through PCI-compliant payment gateways. The Australian Museum does not store complete credit card details on our ICT systems. Guidelines are provided to staff for processing credit card information and banking details.

The Australian Museum collects banking and superannuation information as required for payroll processing, supplier and vendor payments, visitor and member reimbursements.

Access to financial information is restricted to authorised personnel who require it for legitimate business purposes.

2.12. Photography and digital images

The Australian Museum's collection includes photographic and archival materials that may contain images of identifiable individuals, including historical photographs, field research records, and cultural objects. Some of these materials have been or are being digitised as part of the AM's collection management programs. The AM also takes photographs and video footage at events, exhibitions, and public and education programs, which may capture images of identifiable individuals including visitors, members, and program participants. Individuals are notified of photography at events and programs through signage and event communications, and may request that images of them not be taken or used. Where collection materials or event photography contain images of identifiable individuals, the AM has policies and procedures to manage access to, use and disclosure of those images.

2.13. Security systems and surveillance

The Australian Museum collects personal information, including visual images of individuals, through security systems installed in public areas of the Museum and designated workspaces such as loading docks and key access points. This collection is necessary for ensuring the safety of visitors, staff, and the Museum's collections. In certain work locations, surveillance technologies such as cameras, computer monitoring, or tracking devices may be used in accordance with the Workplace Surveillance Act 2005. When workplace surveillance is implemented, employees receive written notification detailing the type of surveillance being

used, how it will be conducted, commencement timing, whether it will be continuous or intermittent, and its duration, as required under the Workplace Surveillance Act 2005.

3. How We Handle Personal and Health Information

The Australian Museum is committed to complying with the Information Protection Principles (IPPs) under the PPIP Act and the Health Privacy Principles (HPPs) under the HRIP Act. This section explains how we implement these principles in practice.

3.1. Lawful Collection (IPP1)

The Australian Museum only collects personal information for lawful purposes that are directly related to its objects and powers under the Australian Museum Trust Act 1975 (NSW). We commit to transform the conversation around climate change, the environment and wildlife conservation, to prioritise First Nations cultures, and to continue to develop world leading science, collections, exhibitions, and education programs. The Australian Museum's statutory powers are outlined in section 8 of the Australian Museum Trust Act 1975 (NSW). They include (among others):

- Procuring and preserving specimens and scientific data relating to the natural sciences
- Promoting and providing exhibits, lectures, films, publications and other educational instruction relating to the natural sciences
- Providing scientific information to the public and to museums or scientific bodies
- Undertaking scientific research in the natural sciences
- Carrying out surveys and other research for statutory bodies and other persons
- Permitting use of the Australian Museum for activities of an educational or cultural nature, including exhibitions, public programming and events
- Engaging in commercial activities in furtherance of the Australian Museum's objects.

The Australian Museum also collects and uses personal information to manage relationships with visitors, members, and donors and to carry out its administrative and employment functions, including under the Government Sector Finance Act 2018 (NSW) and Government Sector Employment Act 2013 (NSW).

3.2. Direct Collection (IPP 2)

Wherever possible, the Australian Museum collects personal information directly from the individual concerned. There are circumstances where indirect collection may occur, such as:

- When the individual authorises collection from someone else and consents to the transfer of their information to the Australian Museum (for example, where an individual consents to the collection of their personal information by a third-party ticketing supplier engaged to sell tickets to an Australian Museum exhibition, or a third-party sponsor or partner)
- When collecting information from parents or guardians about children (for example, in connection with school holiday and educational programs)
- When receiving information from other government agencies for specified purposes

- When conducting donor profiling or wealth screening for fundraising purposes, where personal information collected by third-parties and/or aggregated from publicly available sources may be combined with personal information collected directly by the Museum.

In cases of indirect collection, the Australian Museum manages privacy risks through appropriate safeguards including by requiring staff to conduct a Privacy Impact Assessment prior to the activity. This requirement is embedded in the Australian Museum's policies.

The Australian Museum takes additional care when collecting personal information about children and young people, including in connection with education programs, school group visits, and public programs. Where personal information is collected about children under the age of 16, the AM seeks consent from a parent or guardian wherever practicable. Personal information about children and young people is only collected to the extent necessary for the relevant program or activity and is not used for any secondary purpose, including direct marketing, without parental or guardian consent.

3.3. Notification (IPP 3) and Transparency (IPP 6)

When collecting personal information, the Australian Museum takes reasonable steps to inform individuals:

- That their personal information is being collected
- The purposes for which the information is being collected
- The intended recipients of the information
- Whether the supply of information is voluntary or required by law
- The consequences of not providing the information
- How they can access and correct their information

This notification is provided through the Australian Museum's Privacy Statement available on the Australian Museum's website and privacy notices on forms, ticketing sites, signage, and verbally where appropriate.

3.4. Relevance (IPP 4)

The Australian Museum takes reasonable steps to ensure that personal information it collects is relevant, accurate, complete, up-to-date and not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.

This is achieved through review of databases, collection forms and processes to ensure only necessary information is requested and retained.

3.5. Storage and Security (IPP 5)

IPP 5 and HPP 5 require the safe storage (security) of personal information. The Australian Museum applies appropriate technical and organisation security measures to protect personal and health information, including through:

- Password protection and encryption of electronic records

- Access controls limiting staff access to personal information databases on a need-to-know basis
- Secure physical storage of paper records and archives
- Staff training on information security and privacy compliance
- Security audits and updates to security systems as required.

All staff are required to comply with the Australian Museum's policies and procedures relating to information security and access management, including requirements governing access to personal information held in the Australian Museum's ICT systems.

If personal information managed by the Australian Museum is held or stored by a third party (such as an ICT service provider), the Australian Museum ensures that contracts are entered into with the supplier in accordance with NSW Government mandated arrangements for procuring ICT goods and services, with appropriate clauses requiring the supplier to protect and safeguard the personal information.

Personal information is retained for the period required by the State Records Act 1998 (NSW) and relevant retention and disposal authorities. The retention and disposal of records is managed by a designated Records Manager in accordance with the AM Records Management Policy.

The Australian Museum's Data Breach Policy provides a framework to address any unauthorised access to, or disclosure of personal information.

3.6. Access and Accuracy (IPPs 7-9)

Individuals may (a) enquire about whether the Australian Museum holds their personal information and how it is used, (b) request access to that information, or (c) update their information and preferences, by emailing privacy@australian.museum or submitting a formal application under the PPIP Act.

The Museum will endeavour to provide individuals with access to their personal information as required under the PPIP Act and will make requested amendments without excessive delay or expense. However, in some circumstances, access may be refused in accordance with the PPIP Act.

3.7. Use and Disclosure (IPPs 10-12)

The Australian Museum only uses personal information for the purpose for which it was collected, or a directly related purpose that the individual would reasonably expect.

The Museum will not use personal information for a secondary purpose unless:

- The individual has consented
- The use is for a directly related purpose and the individual would reasonably expect such use
- The use is necessary to prevent serious and imminent threat to life or health
- The use is permitted by law or for law enforcement purposes.

The Australian Museum does not disclose personal information to third parties unless:

- The disclosure is directly related to the purpose for which the information was collected, and the Museum has no reason to believe the individual would object;
- The individual has been made aware that this kind of information is usually disclosed to the recipient;
- The individual has consented to the disclosure;
- The disclosure is necessary to prevent a serious and imminent threat to life or health;
or
- The disclosure is permitted by law or for law enforcement purposes.

3.8. Safeguards on Disclosure (IPP 12)

The Australian Museum has established specific processes for the authorised disclosure of personal information where necessary. Personal information will only be disclosed to third parties in accordance with the requirements of the PPIP Act. Specific disclosure arrangements, including the safeguards that apply to those disclosures, are set out in Section 4 of this Plan.

The Australian Museum does not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities without consent, unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person. These measures ensure that sensitive personal information is only handled and disclosed in accordance with the requirements of IPP 12.

Disclosures of personal information by the Australian Museum to a person or organisation in a jurisdiction outside of New South Wales requires legal input prior to disclosure to ensure compliance with the requirements of section 19 of the PPIP Act and IPP 12.

4. Specific Disclosure Arrangements

If personal information will be disclosed to a third party that is not a NSW Government agency, the Australian Museum requires that:

- A Privacy Impact Assessment is carried out prior to any new disclosure to a third party
- Only the minimum necessary information is disclosed
- The recipient of the information enters into a contract with clauses protecting the use and disclosure of personal information by the recipient and requiring compliance with applicable privacy legislation
- Secure methods of transfer are used.

4.1. Third Party Service Providers

From time to time, the Australian Museum may need to disclose personal information to third-party suppliers providing services to the Museum, including:

- ICT service providers
- Marketing and communications service providers

- Event management services
- Ticketing suppliers
- Customer relationship management system providers.

The Australian Museum uses Tessitura as our customer relationship management and ticketing system through a consortium arrangement managed by the Sydney Opera House Trust. Personal information including membership records, contact details, ticket purchase history, event registration, fundraising and donor data is processed through Tessitura.

4.2. Other Government Agencies

From time to time, the Australian Museum may need to disclose personal information to other NSW Government agencies and departments in connection with its administrative and statutory functions, and to Commonwealth agencies and government agencies in other states. This may include disclosure to the Department of Creative Industries, Tourism, Hospitality and Sport (DCITHS) where it is exercising its governance or oversight functions, and to other agencies where required by law or necessary for the AM's functions. For example, the AM may be required to provide personal information to the Queensland National Parks & Wildlife Service as part of the AM's emergency response protocols for Liard Island Research Station.

The AM also provides anonymised and aggregated workforce diversity data to DCITHS and the Public Service Commission in response to the annual workforce diversity survey.

Personal information of employees, contractors, and suppliers is disclosed to the Department of Customer Service through myWorkZone. myWorkZone involves the handling of personal information of employees (such as their names, date of birth, contact details, bank account details, emergency contact details, job title, line manager, leave balances and possession of work laptops), suppliers (such as the contact and bank account details of any sole traders) and creditors (such as any outstanding fees owed by an individual to the AM).

This disclosure is necessary for the Australian Museum's administrative functions and is carried out in accordance with the PPIP Act and the Privacy Commissioner's Direction under s. 41(1) of the PPIP Act in relation to myWorkZone.

Where personal information is disclosed to NSW Government agencies on an ongoing basis, the Australian Museum seeks to ensure that appropriate documentation is in place, such as a memorandum of understanding or data sharing agreement, that sets out how personal information will be handled and protected by the receiving agency.

4.3. Australian Museum Foundation

The Australian Museum Foundation (AMF) is a not-for-profit organisation that exists solely to raise funds to enable the Australian Museum to achieve its mission. Personal information collected by the Australian Museum may be disclosed to the Australian Museum Foundation for fundraising purposes, including:

- Donor communications
- Invitations to events and exhibitions
- Administrative and profiling purposes
- Relationship management

This disclosure supports the Australian Museum's fundraising activities and is subject to appropriate privacy safeguards. The Australian Museum has a documented protocol with the Australian Museum Foundation which governs the use and access to personal information by the Foundation and requires the Foundation to comply with applicable privacy legislation. Personal information that is collected or used by the Foundation is managed in accordance with the Foundation's Privacy Policy and governed by the Privacy Act 1988 (Cth) and the Australian Privacy Principles.

Individuals can opt out of having their personal information shared with the Foundation at any time by emailing privacy@australian.museum.

5. Health Information

The Australian Museum collects health information only when necessary for AM's functions. The AM complies with the Health Privacy Principles (HPPs) under the HRIP Act in handling this information. Health information is collected directly from the individual wherever practicable, used for the purpose for which it was collected or directly related purposes, and only disclosed in limited circumstances where necessary and relevant to collection purposes, consented to, or required or permitted by law. Individuals are notified of the purpose for which their health information is being collected at the time of collection, including through privacy notices on relevant forms and communications.

Health information is stored securely with restricted access and protected with additional safeguards for sensitive data, and retained in accordance with applicable records retention requirements.

Individuals can access or request amendments to their health information by contacting People & Culture or emailing privacy@australian.museum.

The Australian Museum does not assign unique identifiers to individuals for the purposes of managing health information and does not use identifiers assigned by other organisations. Health information is anonymised where practicable, and the AM ensures appropriate protections are in place if transferring health information outside NSW in accordance with the HRIP Act. The Australian Museum does not use health records linkage systems.

The measures outlined above are designed to ensure compliance with the Health Privacy Principles (HPPs) under the HRIP Act, including in relation to collection, storage, access, use and disclosure of health information.

Where AM employees are based in other Australian states or territories, health information may be disclosed to relevant third parties, including workers' compensation insurers, as required or permitted by the applicable laws of that jurisdiction.

6. Artificial Intelligence

The Australian Museum uses artificial intelligence (AI) tools to support its operations. The AM recognises that AI tools present specific privacy risks. To manage these risks, the AM has implemented the following safeguards:

- Staff are prohibited from uploading or entering personal information or health information into AI tools.

- AI tools that interface with AM ICT systems are configured to ensure they do not access or process personal information or health information held by the AM.
- Where new AI tools are proposed for use at the AM, the AM follows the NSW Government AI Assessment Framework and AI Ethics Policy to assess privacy, ethical, and security risks prior to procurement or implementation.
- A Privacy Impact Assessment is required prior to the implementation of any new AI tool that may involve the collection, use, storage or disclosure of personal information or health information.

7. Special Provisions, Relevant Legislation and Public Registers

7.1. Codes of Practice and Public Interest Directions

The Australian Museum complies with applicable Privacy Codes of Practice and Public Interest Directions issued by the Privacy Commissioner, including the Direction under s. 41(1) of the PPIP Act in relation to myWorkZone. The NSW Public Service Commission has a [Privacy Code of Practice for the Public Service Commission](#) to allow analysis and reporting about employment characteristics. The Australian Museum provides personal information to the NSW Public Service Commission for this purpose.

7.2. Relevant Legislation

Personal information is governed by the PPIP Act and health information is governed by the HRIP Act. The following legislation also interacts with the Acts and impact how the Australian Museum handles personal information:

- Government Information (Public Access) Act 2009 (NSW)
- Australian Museum Trust Act 1975 (NSW)
- Work Health and Safety Act 2011 (NSW)
- Government Sector Employment Act 2013 (NSW)
- State Records Act 1998 (NSW)
- Workers Compensation Act 1987 (NSW)
- Workplace Injury Management and Workers Compensation Act 1998 (NSW)
- Anti-Discrimination Act 1977 (NSW)
- Disability Discrimination Act 1992 (Cth)

7.3. Public Registers

The Australian Museum does not maintain any public registers containing personal information as defined by the PPIP Act.

8. Data Breach Management

The Australian Museum follows the mandatory notification data breach scheme requirements in Part 6A of the PPIP Act and has implemented a Data Breach Policy which includes a data breach response plan. The Data Breach Policy outlines procedures for:

- Identifying and containing data breaches

- Assessing the risk of harm to affected individuals and whether an “eligible data breach” has occurred as defined in section 59D of the PPIP Act
- Notifying the NSW Privacy Commissioner if an “eligible data breach” has occurred
- Notifying affected individuals when appropriate
- Reviewing incidents and implementing preventative measures.

The Australian Museum's Data Breach Policy can be accessed on the staff intranet (Amplify), the Australian Museum website or by request by emailing privacy@australian.museum.

9. Complaints and Review Processes

9.1. Internal Review Rights and Procedures

Individuals have the right to request an internal review if they believe the Australian Museum has breached their rights under the PPIP Act or IPPs, the HRIP Act or HPPs, or a privacy code of conduct. The Australian Museum encourages individuals to try to resolve privacy issues informally before going through the review process, or to contact the AM Legal team to discuss the issue before lodging an internal review.

The internal review process is as follows:

- Submit a written request for internal review to the Director & CEO within 6 months of becoming aware of the breach.
- The Director & CEO will instruct the AM Legal Team to notify the NSW Privacy Commissioner of the internal review request, as required under s54(1) of the PPIP Act and will keep the NSW Privacy Commissioner informed of the progress reports of the internal review.
- A review will be conducted by the AM Legal team or another staff member with sufficient seniority who is not involved in the matter.
- The review will be completed within 60 days of the request and written notification of the outcome will be provided to the individual.
- The notification will also specify findings of the review (and the reasons for those findings), action proposed to be taken by the Australian Museum (and the reasons for taking that action), the right of the individual to have those findings, and the AM's proposed action, administratively reviewed by NCAT.

9.2. Informal Complaint Resolution

The Australian Museum encourages the informal resolution of privacy concerns where appropriate. Individuals with privacy concerns can email privacy@australian.museum or contact the AM Legal Team or submit feedback through the Museum's general feedback channels. Staff can also raise privacy concerns directly with their manager or Executive Leadership Team Member.

9.3. Role of the Privacy Commissioner

Individuals have the right to make a complaint directly to the NSW Privacy Commissioner at any time by contacting the Information and Privacy Commission NSW at the contact details set out in Section 13 of this Plan.

The Privacy Commissioner must be informed of all internal review applications, and may make submissions to the Museum about the internal review. The Privacy Commissioner can also provide advice to individuals about their review rights.

9.4. External Review by NCAT

If an individual is not satisfied with the outcome of an internal review, they can apply to the NSW Civil and Administrative Tribunal (NCAT) for an external review. Applications to NCAT must be made within 28 days of being notified of the internal review outcome.

10. Implementation and Compliance

10.1. Privacy Officer Functions

Responsibility for privacy compliance under the PPIP Act and HRIP Act rests with the Director & CEO as the accountable officer of the Australian Museum. The AM Legal team exercises the Privacy Officer functions in the ordinary course on behalf of the Director & CEO, including managing privacy complaints and internal review applications, monitoring communications to privacy@australian.museum, advising staff on privacy obligations, liaising with the Information and Privacy Commission, and maintaining and reviewing this Privacy Management Plan.

The People & Culture team manages personal and health information in connection with employment matters with input from the AM Legal team as required.

10.2. Training and Awareness

The Australian Museum promotes privacy awareness and compliance through a range of measures:

- The Executive Leadership Team reinforces compliance by endorsing this Plan and making it publicly available, reviewing and updating the Plan every three years (or earlier if necessary) and reporting on privacy issues in the DCITHS's Annual Report.
- This Plan is published on the intranet to ensure staff are aware of their rights and obligations in relation to privacy.
- Staff are provided training on the AM Code of Conduct on induction, which includes responsibility to protect personal information and health information and comply with applicable privacy legislation.
- Privacy training modules are available to all staff and volunteers through the AM's learning and development platform. Staff whose roles involve the collection, use, storage or disclosure of personal information are encouraged to complete relevant training modules.
- Privacy compliance requirements are embedded in AM policies and procedures that staff are required to comply with, including the Procurement and Contract Management Policy, the AM Code of Conduct.
- The AM Legal team provides training and advice on privacy compliance to AM staff on request and circulates guidance notes and updates about changes to privacy legislation and procedures as required.
- Privacy guidance materials and template contracts are available on the staff intranet (Amplify).

10.3. Privacy Impact Assessments

Australian Museum staff are required to conduct a Privacy Impact Assessment for any new project that involves the collection or handling of personal information, or any new use or disclosure of personal information (e.g. if personal information will be used for a secondary purpose or disclosed to a third party). A Privacy Impact Assessment must also be conducted when significant changes are proposed to ICT systems, security systems and other technologies are implemented that may impact privacy.

10.4. Public Education Initiatives

The Australian Museum promotes privacy awareness to the public through:

- Display of Privacy Statement on the Australian Museum website
- Privacy notices on forms and at the point of collection of personal information
- Contact details for privacy @australian.museum are publicly displayed to manage privacy compliance and respond to requests and correspondence relating to privacy
- Transparency about information handling practices and procedures for accessing and correcting personal information as set out in this Privacy Management Plan.

10.5. Compliance Auditing

The Australian Museum regularly reviews its information handling practices, privacy complaints and data breaches to identify and address any systemic issues. Contracts with third parties that involve the collection, use or disclosure of personal information require legal review prior to signing to ensure compliance with privacy legislation.

10.6. Breaches and Offences

All Australian Museum employees, contractors, and volunteers must comply with this Privacy Management Plan and applicable privacy legislation. Breaches of privacy obligations, including unauthorised access to or disclosure of personal information, failure to follow proper procedures, or accessing information without legitimate business purpose, may constitute misconduct subject to disciplinary action and potentially termination of employment. It is also an offence under applicable privacy legislation to intentionally misuse or unlawfully disclose personal or health information.

Staff must immediately report any actual or suspected privacy breaches to their manager, the Privacy Officer, or a Disclosure Officer pursuant to the AM's Public Interest Disclosure Policy. Failure to report known breaches may itself constitute misconduct.

Under the PPIP Act and HRIP Act, it is a criminal offence, punishable by up to two years' imprisonment, for a staff member to intentionally use or disclose any personal information about another person, to which the employee has or had access in the exercise of his or her official functions (except as necessary for the lawful exercise of his or her official functions).

Part 8 of the PPIPA and part 8 of the HRIPA provide further details about offences in respect of personal and health information. These parts also provide certain protections from liability where a person has acted in good faith.

11. Related Policies and Procedures

The Australian Museum's policies and procedures are developed and reviewed to ensure that privacy compliance obligations are embedded in the AM's operations and decision-making.

The following policies and procedures support the Australian Museum's privacy framework:

- AM Access Management Policy
- AM Acceptable Use Policy
- AM Information Security Policy
- AM Records Management Policy
- AM Data Breach Policy
- AM Code of Conduct
- AM Conflict of Interest Policy
- AM Gifts and Benefits Policy
- AM Privacy Statement
- Public Interest Disclosure Policy
- AM Procurement and Contract Management Policy
- AM Travel and Field Work Policy
- AM Volunteer Policy
- AM WHS Policy
- AM Respectful, Inclusive and Fair Workplace Policy
- AM Sexual Harassment Prevention Policy
- AM Workplace Adjustment Policy
- Office Ergonomics Framework
- NSW Premier & Cabinet Procedures for Managing Non-Work Related Injuries or Health Conditions
- AM Emergency Management Plan

These policies can be accessed on the AM staff intranet (Amplify). The AM Privacy Statement is made available to the public on the Australian Museum website.

12. Definitions and abbreviations

- **HRIP Act:** Health Records and Information Privacy Act 2002 (NSW)
- **HPPs:** Health Privacy Principles
- **IPPs:** Information Protection Principles
- **PIIP Act:** Privacy and Personal Information Protection Act 1998 (NSW)

13. Contact Information

Australian Museum Privacy Officer

c/o General Counsel
Australian Museum Legal Team
Australian Museum
1 William Street Sydney NSW 2010
Email: privacy@australian.museum

Information and Privacy Commission NSW

Information and Privacy Commission
NSW Level 15, McKell Building
2-24 Rawson Place
Sydney NSW 2000
Email: ipcinfo@ipc.nsw.gov.au
Phone: 1800 IPC NSW (1800 472 679)
Website: www.ipc.nsw.gov.au

NSW Civil and Administrative Tribunal

NSW Civil and Administrative Tribunal (NCAT) Administrative and Equal Opportunity Division
Level 10, John Maddison Tower, 86-90 Goulburn Street Sydney NSW 2000 Phone: 1300 006
228 Website: www.ncat.nsw.gov.au

14. Accessibility and Review

Availability of the Plan

This Privacy Management Plan is available on the Australian Museum staff intranet. It can be provided in hard copy upon request from the AM Legal Team.

Version and Review Dates

Version	Date	Approved by:
1.0	25 June 2026	Director & CEO

Next review date: 3 years from approval, or sooner if required due to operational or legislative changes.