



WESTERN
AUSTRALIAN
MUSEUM

Information Breach Policy

Version Control

Version	2.0
Approved by	Board of Trustees
Date effective	<i>1 July 2026</i>
Document owner	Director, Corporate and Strategy, CFO
Rescissions and replacements	NA
Next review date	<i>May 2028</i>
Museum Records Folder No.	22/533
Contact for queries	Manager Records, Amrik Singh

Information Breach Policy

Contents

1. PURPOSE	3
2. DEFINITIONS	3
3. POLICY STATEMENT	3
4. SCOPE	4
5. RESPONDING TO INFORMATION BREACHES	4
5.1 Containment and mitigation	5
5.2 Assessment	5
5.2.1 Assessing the likelihood of serious harm	6
5.3 Notification	6
5.3.1 Voluntary notification	7
5.3.2 Breaches involving other entities	8
5.3.3 Shared information	8
5.3.4 Review and Improve	9
6. RECORDKEEPING AND REPORTING	9
7. HOW TO REPORT A SUSPECTED INFORMATION BREACH	9
8. INTERACTION WITH OTHER OBLIGATIONS	10
9. REVIEW OF THIS POLICY	10
10. REVISION HISTORY	11

1. PURPOSE

This policy sets out how the Western Australian Museum (the Museum) prevents, identifies and responds to information breaches in accordance with the *Privacy and Responsible Information Sharing Act 2024* (WA) (PRIS Act).

The Museum is committed to protecting personal information, minimising harm arising from information breaches, and being appropriately transparent with affected individuals, regulators and other stakeholders.

2. DEFINITIONS

Information breach is an incident involving:

Unauthorised access to information (i.e., someone sees or uses information without permission); or

Unauthorised disclosure of information (i.e., information is shared with someone who shouldn't have it); or

Loss of information in circumstances where unauthorised access or disclosure is likely.

Notifiable Information Breach is where there is unauthorised access, unauthorised disclosure, or loss of personal information which is likely to result in serious harm to any individual to whom the information relates.

Serious harm may include (but is not limited to) physical harm or intimidation, serious psychological or emotional harm, identity theft, financial loss, or reputational damage.

3. POLICY STATEMENT

In delivering services, the Museum inevitably collects information that may reveal information about individuals. This information assists the Museum to better understand and meet individual needs and the needs of the State.

However, the Museum recognises that the personal information it holds and the ways in which it uses that information also carry risks such as:

- loss of seclusion, i.e. the enjoyment of being left alone, as well as controlling who is aware of aspects of an individual's life or identity which they might reasonably consider to be appropriate knowledge only to themselves or other specific individuals;

- loss of personal autonomy that might arise from excessive surveillance or monitoring of an individual's behaviours;
- domestic violence, harassment, loss of reputation or embarrassment where inappropriate access is given to individuals close or known by the affected individual;
- identity theft and financial/property crime;
- loss of trust in institutions (such as the Museum and government generally), making it more difficult for individuals to access the benefits of public services; and
- entrenching of systemic biases and discrimination, e.g. where inappropriate or irrelevant information is collected during a recruitment process and unduly influences decision making.

The Museum is committed to reducing this exposure, including by taking steps to prevent information breaches from occurring. However, where they do occur, the Museum will take reasonable and proportionate steps to:

- contain the breach;
- assess its nature and potential consequences;
- mitigate the risk of harm;
- notify the Information Commissioner and affected individuals where required;
- consider whether voluntary notification is appropriate where notification is not legally required;
- keep appropriate records; and
- review the incident and identify opportunities for improvement.

4. SCOPE

This policy applies to personal information handled by the Museum in connection with its functions, activities, programs and services including personal information handled on behalf of the Museum by third parties such as IT service providers.

Information breaches affecting more than one entity will be managed in consultation with the other entities to clarify responsibilities, coordinate communications and meet applicable legal and contractual obligations.

5. RESPONDING TO INFORMATION BREACHES

The Museum manages information breaches through four principal activities:

1. containment and mitigation;
2. assessment;

3. notification (undertaken where required or appropriate); and
4. review and improvement.

These activities are not necessarily sequential and may be undertaken concurrently or alongside other applicable incident response activities. The nature and extent of the response will depend on the type and circumstances of the breach.

5.1 Containment and mitigation

Where the Museum reasonably suspects that a notifiable information breach may have occurred, it will immediately take all reasonable steps to contain the suspected breach.

The Museum will also take reasonable steps to mitigate harm caused, or potentially caused, by the breach. Depending on the circumstances, this may include:

- securing information or systems;
- recovering information;
- preventing further unauthorised access or disclosure;
- preserving information relevant to the assessment;
- engaging with other entities involved in the breach; and
- identifying measures that affected individuals may take to protect themselves.

Containment and mitigation activities will be undertaken in a manner that avoids unnecessarily increasing the risk of harm.

The PRIS Act requires immediate reasonable containment and reasonable mitigation steps where an entity reasonably suspects a notifiable information breach.

5.2 Assessment

The Museum will assess a suspected notifiable information breach as soon as reasonably practicable and, unless an extension is granted under the PRIS Act, within 30 days after forming the reasonable suspicion.

The assessment will determine whether:

- an information breach occurred;
- personal information was involved;
- unauthorised access or disclosure occurred or is likely to occur;
- serious harm to any affected individual is likely;
- the breach is a notifiable information breach; and

- notification or other protective action is required or appropriate.

The Museum will prepare a written report on the assessment and have regard to any applicable privacy guidelines issued by the Information Commissioner.

5.2.1 Assessing the likelihood of serious harm

In determining whether serious harm is likely, the Museum will consider all relevant circumstances, including:

- the nature of the personal information;
- the sensitivity of the personal information;
- whether security measures protected the information;
- whether those security measures were, or could be, circumvented;
- the persons or kinds of persons who obtained, or could obtain, the information;
- whether those persons may intend to cause harm;
- the nature and severity of the harm that has occurred or could occur;
- the likelihood that potential harm will occur;
- whether remedial action has prevented or reduced the risk of harm; and
- any other relevant matters.

These considerations reflect the serious-harm assessment factors set out in the PRIS Act. The Museum also follows any applicable guidance provided by the Office of the Information Commissioner, relevant case law and other best practice guidance. The Museum is aware of the extensive guidance issued by the Office of the Australian Information Commissioner (**OAIC**) and will follow that guidance with respect to information breaches involving Tax File Numbers (where notification of the OAIC may be required). The Museum will otherwise be guided by that material to the extent it does not conflict with guidance issued by the Office of the Information Commissioner.

5.3 Notification

Where the Museum determines that a notifiable information breach has occurred, or that there are reasonable grounds to believe that one has occurred, the Museum will notify the Information Commissioner in writing as soon as practicable.

The Museum will also take all reasonable steps to notify each affected individual in writing as soon as practicable, subject to any exceptions under the PRIS Act. Exceptions to making notifications under the PRIS Act generally relate to circumstances where notifications might

themselves give rise to a disproportionate risk of serious harm including domestic violence and other threats to health, safety and wellbeing.

As set out below, in many circumstances, the Museum recognises that there may be circumstances where it will be in the best interests of individuals to be notified even where we are not obligated to do so.

A notification to affected individuals will provide information required by the PRIS Act and, where appropriate:

- describe what happened;
- identify the kinds of personal information involved;
- explain the steps the Museum has taken or proposes to take;
- recommend steps affected individuals can take to reduce potential harm;
- provide relevant Museum contact details; and
- explain how affected individuals may make a privacy complaint.

The Museum may update notifications or provide additional information where material facts become known after the initial notification.

5.3.1 Voluntary notification

The Museum recognises that an information breach may warrant communication even where it does not meet the legal threshold for a notifiable information breach.

The Museum may voluntarily notify affected individuals, regulators or other relevant stakeholders where it considers that notification would be reasonable and appropriate in the circumstances.

In deciding whether to make a voluntary notification, the Museum may consider:

- where notification will help an individual to protect themselves from harm even though the harm is not probable;
- whether notification would promote transparency, accountability and public trust;
- whether the information would have an educational or protective benefit for affected individuals;
- the reasonable expectations of affected individuals;
- the nature and sensitivity of the information;
- whether notification could cause unnecessary distress or confusion;
- whether notification could increase the likelihood or severity of harm;

- the risk of notification fatigue (i.e. making individuals inert to more serious data breach notification by inundating them with less serious ones);
- the possible impact on the safe and effective delivery of public services;
- communications by other entities involved in the breach; and
- any other relevant legal, regulatory, safety or public-interest considerations.

A decision not to make a voluntary notification does not prevent the Museum from taking other actions to contain the breach, mitigate risk, improve its practices or engage with relevant regulators.

This approach reflects the Museum's framework, which balances transparency, trust and opportunities for individuals to protect themselves against risks such as unnecessary distress, increased harm and notification fatigue.

5.3.2 Breaches involving other entities

Where an information breach involves a contracted service provider, another public entity, a partner or another third party, the Museum will consider:

- each entity's legal and contractual obligations;
- which entity is best placed to notify affected individuals;
- the need for consistent and timely communications;
- the risk of duplicative or conflicting notifications; and
- the steps required to contain the breach and prevent further harm.

The Museum will seek to coordinate its response with the other entities while independently meeting its own legal obligations.

5.3.3 Shared information

The responsible information sharing framework is a voluntary purpose limited framework established under the PRIS Act for sharing information safely and appropriately between WA public sector bodies and limited other bodies undertaking work aligned to public services.

Where an information breach involves information shared under the responsible information sharing framework established, the Museum will take the steps required under that framework with respect to information breaches. These may include containment, assessment and mitigation, as well as notification to the provider of the information and the Chief Data Officer where required.

5.3.4 Review and Improve

Following an information breach, the Museum will review the circumstances of the incident and the effectiveness of its response.

The review may consider:

- the root cause/s of the breach;
- whether the incident was identified and escalated promptly;
- the effectiveness of containment and mitigation measures;
- whether communications were timely, clear and appropriate;
- whether policies, practices and safeguards operated as intended;
- whether similar information may be exposed to comparable risks;
- actions required to prevent or reduce the likelihood of recurrence; and
- opportunities to improve the Museum's information handling, security, recordkeeping, privacy practices and incident management.

6. RECORDKEEPING AND REPORTING

The Museum maintains an Information Breach Register recording details of all reported information breaches, the kind of breach, steps taken to contain the breach and mitigate the risk, assessment outcomes, details of notifications made to the Information Commissioner and affected individuals, any remedial actions taken to prevent future breaches, and the estimated cost of the breach.

All records submitted or created in the management of information breaches will be managed in accordance with the State Records Act 2000 (WA) and our Record Keeping Plan.

7. HOW TO REPORT A SUSPECTED INFORMATION BREACH

Anyone who believes that personal information handled by the Museum may have been accessed, disclosed or lost without authority may contact the Museum using the privacy contact details published in the Museum Privacy Statement.

Reports should include sufficient information to help the Museum understand the concern but should not include unnecessary copies of personal or sensitive information.

The Museum will handle reports in accordance with this policy and any applicable legal requirements.

8. INTERACTION WITH OTHER OBLIGATIONS

This policy operates alongside the Museum's:

- Privacy Statement;
- information security policies and standards;
- records management policies and plans;
- incident management arrangements;
- contractual obligations; and
- other applicable legal and regulatory obligations.

An incident may give rise to obligations under more than one legislative or regulatory framework. The Museum will consider and manage those obligations as part of its response.

Nothing in this policy limits the application of:

- the PRIS Act;
- an applicable secrecy provision or other written law;
- a lawful direction or requirement of a regulator;
- a court or tribunal order; or
- another legal obligation applying to the Museum, including obligations with respect to personal information of individuals residing overseas.

9. REVIEW OF THIS POLICY

The Museum will review this policy at least annually and may review it earlier where appropriate.

A review may consider:

- amendments to the PRIS Act or other applicable laws;
- regulations, determinations or approved forms made under the PRIS Act;
- privacy guidelines issued by the Information Commissioner;
- guidelines issued by the Chief Data Officer;
- lessons arising from information breaches;
- changes to the Museum's functions, services, risks or operating environment; and
- developments in privacy and information security practice.

10. REVISION HISTORY

Date Reviewed	Version no.	Summary of Changes / Revision	Author
May 2026	V1.0	First draft	Amrik Singh
13/10/2026	V2.0	Update from CITS	Amrik Singh