

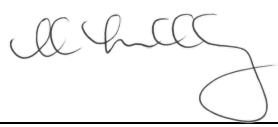
AUSTRALIAN MUSEUM

DATA BREACH POLICY



INFORMATION SECURITY FRAMEWORK

DOCUMENT CLASSIFICATION: OFFICIAL

Effective Date	27 November 2023	Next Review	In 1 year
Approval	Director and CEO 		
Approval Date	27 November 2023		
Accountable Director	Chief Operating Officer		
Responsible Officer	Head of ICT		
Version	1.0		
TRIM No.	D23/34278		

AUSTRALIAN MUSEUM

1 William Street Sydney
NSW 2010 Australia
T 61 2 9320 6000
australianmuseum.net.au





TABLE OF CONTENTS

1	INTRODUCTION	4
2	WHAT IS A DATA BREACH, HOW TO IDENTIFY ONE AND WHEN TO REPORT IT	4
2.1	What is a data breach?	4
2.2	What is an 'eligible data breach'?	5
2.3	What is 'personal information'?	5
2.4	How to identify a data breach?	5
2.5	When to report a data breach?	6
2.6	Where to access further information	6
3	PLAN FOR CONTAINING, ASSESSING AND MANAGING ELIGIBLE DATA BREACHES	6
3.1	Data breach response plan	6
3.2	Other relevant considerations	8
4	ROLES AND RESPONSIBILITIES.....	10
5	RECORD-KEEPING	11
6	MANAGING TRAINING, CONTRCTORS, UPDATES	11
7	REFERENCES	12



1 INTRODUCTION

Amendments to the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) introduced the new Mandatory Notification of Data Breach (**MNDB**) Scheme. The MNDB Scheme requires public sector agencies to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm.

This Data Breach Policy (**Policy**) outlines the procedures for addressing a breach of data held by the Australian Museum (**AM**). This Policy outlines:

- (a) what constitutes a breach, how staff are to identify one and when to report it;
- (b) the plan for containing, assessing and managing an eligible data breach;
- (c) the roles and responsibilities of the AM's Directors, Managers, staff and any other personnel;
- (d) record-keeping requirements; and
- (e) how the AM is managing training, contractors and updates to this Policy.

Effective breach management is essential for the AM to mitigate or avert potential harm to any individuals involved and the AM, and plays a crucial role in preventing future breaches.

2 WHAT IS A DATA BREACH; HOW TO IDENTIFY A BREACH AND WHEN TO REPORT

2.1 What is a data breach?

A data breach is a security incident which results in unauthorised access or use of sensitive, protected, personal or confidential data and information. Some examples of data breaches include:

- (i) loss or theft of unencrypted physical devices (such as laptops and storage devices) or paper records that contain personal information;
- (ii) unauthorised access to personal information such as by someone gaining unapproved access to AM systems and/or emails;
- (iii) inadvertent disclosure of personal information due to 'human error' (for example, an email sent to the wrong person);
- (iv) disclosure of an individual's personal information to a scammer, as a result of inadequate verification procedures.



2.2 What is an ‘eligible data breach’?

An ‘eligible data breach’ occurs when:

1. there has been unauthorised access to, or disclosure of personal information held by a public sector agency, or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to or disclosure of the personal information; **and**
2. a reasonable person would conclude that the access to or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

The examples in paragraph 2.1 will only be considered ‘eligible data breaches’ if they are likely to result in serious harm to an individual.

2.3 What is ‘personal information’?

Personal information is defined in section 4 of the PPIP Act as ‘*information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from information or opinion*’.

The MNDB Scheme also applies to health information which is considered personal information and is defined in section 6 of the *Health Records and Information Privacy Act 2002* as personal information or an opinion about a person’s health, health services that have been provided (or are going to be provided) to a person, and their wishes about future health services.

2.4 How to identify a data breach?

There is no ‘template’ or ‘one-size-fits-all’ for a data breach. It can occur through a range of different means or channels, and can be deliberate (such as a hacker gaining access to the AM’s systems) or accidental (such as inadvertently sending an email to the wrong person).

The most common types of data breaches are caused by human error, for example:

- inadvertently emailing the wrong person;
- falling victim to phishing scams;
- poor password security;
- leaving sensitive documents unattended.

This list is not exhaustive, but is intended to outline the most common scenarios that result in data breaches.



2.5 When to report a data breach?

If you **suspect** there has been a data breach, or are aware that a data breach has occurred, you must immediately report the breach or suspected breach to your supervisor, the AM Legal team, and the Head of ICT. Even if you are unsure whether there has been an actual breach, you must report it.

It is the role of the Legal team and Head of ICT, as part of the Data Breach Response Team, to review the information you have provided and make an assessment about whether there has been an '*eligible data breach*'. This assessment must be undertaken within 30 days. They will then undertake the appropriate course of action.

2.6 Where to access further information

For further information or resources to help you understand any aspect of this Policy, please consult the Head of ICT or use any of the helpful links referred to in section 7 of this Policy.

3 PLAN FOR CONTAINING, ASSESSING AND MANAGING ELIGIBLE DATA BREACHES

3.1 Data breach response plan



Step 1: Alert & Identify

It is the responsibility of all AM employees, volunteers and contractors to remain vigilant and report any data breach or suspected data breach. Any staff member who suspects a data breach may have occurred, having regard to section 2, must promptly alert their supervisor, the Legal Team and the Head of ICT of the suspected breach.

The staff member who discovered the breach should try and provide the following information:

- contact name and number of the person reporting the incident;
- the type of data or information involved;
- location of the incident;
- data and time the incident occurred;
- location of the data or information or equipment affected;
- any other relevant circumstances.



The supervisor, Legal Team and Head of ICT must notify the CEO of the suspected data breach immediately. The CEO will then determine whether the Data Breach Response Team is required to be convened to undertake Steps 2 to 5 below.

Step 2: Contain and Verify

Contain

Once a data breach is identified or suspected, the AM's Data Breach Response Team¹ will take immediate steps to contain the breach. Containment steps will depend on the nature of the breach, but may include shutting down the system affected by the breach and such other steps necessary to mitigate the impact of the breach and the risk of harm to individuals and the AM.

Verify

The Data Breach Response Team will also establish and verify the circumstances of the breach including those details provided by the staff member who alerted the Data Breach Response Team.

Step 3: Assess

Once the breach has been contained and key details have been verified, the Data Breach Response Team will assess the impact of the breach within 30 days, if there are reasonable grounds to suspect there may have been an eligible data breach. This assessment includes considering the following matters:

General matters

- the type of information involved;
- cause of the breach;
- extent of the breach;
- the risk of harm arising from the breach;
- who is affected by the breach;
- the context of the information;

Cause and extent

- whether there is risk of ongoing breaches or further exposure;
- whether there is evidence of theft;
- the source of the breach (accidental vs. intentional);
- has the information been recovered;
- have steps been taken to mitigate any harm;
- is this an isolated incident or a systematic problem;
- how many individuals are affected;

¹ See section 4 for details of the Data Breach Response Team.



Risk of harm to individuals

- who has gained unauthorised access to the affected information;
- how the information could be used;
- the harm likely to occur from the breach, including whether it is serious harm;

Other Risks

- loss of trust in the agency;
- reputational damage;
- legal liability

The IPC has released a [Self-assessment Tool for Mandatory Notification of Data Breach Guidelines](#) which is designed to assist agencies to make assessments on whether an 'eligible data breach' has occurred. The Data Breach Response Team will use this Guideline and consider the above questions to make the relevant assessment.

Step 4: Notify

If the Data Breach Response Team determines that the breach is an eligible data breach or there are reasonable grounds to believe it is an eligible data breach, then it will take steps to notify the affected individual/s and the Privacy Commissioner.

Step 5: Review & Prevent

Once all immediate steps have been taken to contain the breach and mitigate any risk of harm to individuals or the AM, the Data Breach Response Team will review the circumstances of the breach, including:

- what went wrong;
- how the issues are addressed; and
- whether changes are needed to processes and procedures to prevent a similar breach from occurring in the future.

The Data Breach Response Team will report the outcome of its review and make any recommendations to the Executive Leadership Team (ELT) for the prevention of future breaches.

3.2 Other relevant considerations

(a) Incidents involving other entities

Where an incident or data breach involves another entity, such as one collecting information for on behalf of the AM (for example, an IT supplier), the Data Breach Response Team will work with that entity to ensure that the appropriate steps are being taken for the management, prevention and assessment of such an incident.

(b) Reporting to external agencies or entities



The AM may be required to report the incident or data breach to another agency, such as the NSW Police Force (if the breach was due to criminal conduct, for example), the AM's insurer, external legal counsel, Cyber Security NSW and the IPC. The Data Breach Response Team will assess whether the circumstances and nature of the breach require reporting to any external agencies or entities, and will notify and inform those agencies accordingly.



4 ROLES AND RESPONSIBILITIES

The AM's Data Breach Response Team is as follows:

Role	Responsibility
Chief Executive Officer	<ul style="list-style-type: none">• overall accountability for data breaches;• directing the Data Breach Response Team to undertake assessment in accordance with Steps 2 to 5 of the Data Breach Response Plan;• reporting to external agencies, if and when required;• notifying Privacy Commissioner of eligible data breaches; and• maintaining this policy
Head of ICT	<ul style="list-style-type: none">• leading the Data Breach Response Team;• reporting to the ELT;• implementing plans for monitoring, management, containment and prevention of data breaches; and• overseeing AM's cybersecurity program to ensure that it is consistent with industry practice.
Chief Operating Officer	<ul style="list-style-type: none">• reporting to the ELT and CEO;• managing the Data Breach Response Team; and• maintaining this policy
Legal Team	<ul style="list-style-type: none">• assessing legal liability and providing legal advice;• assessing the risks for individuals associated with the breach;• reporting to the ELT and CEO;• reporting to external agencies, if and when required;• assisting with development of strategies to manage, contain and prevent data breaches;• assisting with notifications to individuals affected by eligible data breaches;• assisting with notifications to the Privacy Commissioner of eligible data breaches; and• drafting clauses for contracts with suppliers to require notification of data breaches and compliance with applicable legislation.
ICT Team	<ul style="list-style-type: none">• implementing plans for management, containment and prevention of data breaches;• reviewing and managing ICT and cyber security measures;• collecting and providing information relating to the breach;• monitoring controls including assistance with log collection for access, authentication, IDS/IPS, firewalls, antivirus software etc.; and



	<ul style="list-style-type: none">• acting at the direction of the Head of ICT to avoid or mitigate the data breach.
People & Culture	<ul style="list-style-type: none">• providing clear communications to staff about the breach;• facilitating training to staff about policies and procedures to prevent data breaches;• encouraging staff to be proactive about data security and protection; and• assisting with notifications to individuals affected by eligible data breaches.
Media & Communications Team Member	<ul style="list-style-type: none">• assisting with notifications to individuals affected by eligible data breaches;• assisting with notifications to the Privacy Commissioner of eligible data breaches;• monitoring and assessing media channels; and• reporting to the public and media about any eligible data breaches.

5 RECORD-KEEPING

The AM will retain all records relating to data breaches and incidents in accordance with its Records Management Policy and will record such incidents on its internal register.

The AM also has a Public Notification Register on which it will register any notifications made under the PPIP Act of eligible data breaches. The Public Notification Register is available on the AM Website.

6 MANAGING TRAINING, CONTRACTORS, UPDATES

All AM employees and contractors are required to complete regular mandatory privacy training and cyber security training to raise awareness and understanding of the AM's privacy and cyber security obligations, including in relation to data breaches. This training is also provided as part of induction processes.

All AM contractors are subject to privacy obligations, including requirements to handle data breaches in accordance with the PPIP Act and to immediately notify the AM of any data breach or suspected data breach.

The AM will review and test this Policy annually.



7 REFERENCES

Definitions	
AM Website	means https://australian.museum .
Data Breach Response Team	means the AM staff who are responsible for containing, managing and assessing any data breaches that may occur at the AM. The roles are identified at section 4 of this Policy.
Eligible data breach	has the meaning given to it under section 59D of the PPIP Act, as outlined in section 2.2 of this Policy.
ELT	means the Executive Leadership Team of the Australian Museum, consisting of: <ul style="list-style-type: none">• Director and Chief Executive Officer;• Chief Operating Officer;• Chief Financial Officer;• Chief Experience Officer;• Chief Scientist and Director of AMRI;• Director of First Nations;• Director of Marketing Communications & Partnerships;• Director of Public Affairs & Development; and• Associate Director of People & Culture.
IPC	means the Information and Privacy Commission of New South Wales.
MNDB Scheme	means the Mandatory Notification of Data Breach Scheme under the PPIP Act.
Personal information	has the meaning given to it under section 4 of the PPIP Act, as outlined in section 2.3 of this Policy.
PPIP Act	means the <i>Privacy and Personal Information Protection Act 1998</i> (NSW) as amended and in force on 28 November 2023.
Privacy Commissioner	means the Privacy Commissioner at the IPC.
Supporting Information	
Legislative Compliance	<i>Privacy and Personal Information Protection Act 1998</i> (NSW) <i>Health Records and Information Privacy Act</i> (NSW) <i>Privacy and Personal Information Regulation 2014</i> (NSW) <i>Privacy and Personal Information Amendment Bill 2022</i> (NSW)



Helpful Information	<p>Resources on IPC's website, including:</p> <ul style="list-style-type: none">• <u>Fact Sheet for agencies: Exemptions from notification to affected individuals</u>• <u>Guide to managing data breaches in accordance with the PPIP Act</u>• <u>Form: Data Breach Notification to the Privacy Commissioner</u>• <u>Guide to Regulatory Action under the MNDB Scheme</u>• <u>Guideline - Guidelines on the assessment of data breaches under Part 6A of the PPIP Act</u>• <u>Guideline - Guidelines on the exemption for risk of serious harm to health or safety under section 59W</u>• <u>Guideline - Guidelines on the exemption for compromised cyber security under section 59X</u>• <u>Data Breach Self-assessment Tool for MNDB</u>
Supporting Documents	Privacy Management Plan
Related Documents	Acceptable Use Policy Information Security Policy Access Management Policy Records Management Policy