STATE LIBRARY
QUEENSLAND

Data Breach Policy

File number	635/380/009
Maintained by	Compliance and Assurance
Approval date	October 2025
Next review date	October 2026

1. Introduction

State Library of Queensland (State Library) understands that visitors and users of our website & services are concerned about their privacy and the confidentiality and security of information that is provided to us.

State Library is committed to protecting your privacy. Full details of how we collect, protect and manage your personal information, and how we will respond should breaches of data occur, may be found on our Privacy Page (https://www.slq.qld.gov.au/privacy).

2. Authority

This policy is applied by the authority of the State Librarian and CEO (SLCEO).

3. Policy statement

State Library is required to deal with personal information in compliance with the Information Privacy Act 2009. Chapter 3A of the Information Privacy Act 2009 (IP Act) creates a Mandatory Notification of Data Breach (MNDB) scheme.

The MNDB Scheme requires State Library to take actions in relation to suspected and confirmed eligible data breaches.

State Library shall notify the Office of Information Commissioner (OIC) and affected individuals of eligible data breaches unless an exemption applies.

State Library takes proactive steps to contain, assess and mitigate data breaches as outlined in this Policy, the Information Security Incident Response Plan, the Business Continuity Plan, the Data Breach Response Plan and other related State Library policies and procedures.

4. Purpose

The purpose of this policy is to provide an overview of State Library's processes in relation to containing, assessing, managing, notifying and reporting on eligible data breaches in accordance with the MNDB Scheme. This policy complies with section 73 of the Information Privacy and Other Legislation Amendment Act 2023 (IPOLA) and Chapter 3A of the IP Act.

Employees should consult State Library's Data Breach Response Plan for detailed guidance on how to respond to a data breach.

5. Scope

Compliance with this policy is required by:

- all State Library permanent full time, part time, volunteer, trainee and temporary employees and personnel authorised to access State Library information systems and assets
- any consultants and persons or organisations authorised to administer, develop, manage and support State Library Information systems and assets
- third party suppliers, vendors and hosted/managed service providers.
- Library Board and other committee members and Queensland Library Foundation Councillors.

6. Responsibilities

Word	Definition
All staff	• Report a suspected data breach as soon as they suspect, or are first aware of, the breach as required under the MNDB Scheme • Take immediate steps to contain a data breach, including advising relevant staff who can take immediate action • Cooperate with, participate in and support containment, response, assessment or a post-breach review under this policy where required to do so, including the provision of accurate and honest information. Where staff are directly involved in a data breach incident, procedural fairness will be observed in accordance with the State Library's performance and conduct management policies. • Comply with recordkeeping obligations
Executive Leadership Team/Senior Leadership Team	• Immediately report a cyber security incident that is also a data breach to the Lead, Information Security, if not already reported. • Where relevant, notify the Information Commissioner, affected persons and others where required. • Implement the Cyber Security Incident Response Plan and related procedures if the data breach is also a cyber security incident. • Convene the Data Breach Response Team, when appropriate
Directors, Managers and People Leaders	• Identify and escalate concerns within area of responsibility which may enliven the requirements of this Data Breach Policy. • Immediately report a data breach that is also a cyber security incident to the Service Desk or Lead, Information Security, if not already reported.
Contract Managers	• Ensure that all contracts the involve the sharing or management of personal information include clauses binding vendors to the MNDB Scheme.

7. Definitions

Word	Definition
Approved User	Any State Library employee, volunteer, contracted service provider, graduate, consultant, vendor engaged by State Library and any other authorised individual accessing State Library systems, networks and or information.
Cyber Incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
Data Breach	When personal information held by State Library is lost or subject to unauthorised access or disclosure.
Data Breach Response Plan	A detailed plan outlining the steps required for State Library employees to contain, assess, investigate and respond to a data breach.
Data Breach Response Team	A team (led by Executive Director Corporate Services (EDCS) and consisting of senior State Library personnel responsible for coordinating State Library's response to a data breach.
Eligible Data Breach	A data breach likely to result in serious harm to affected individuals, considering the likelihood of harm occurring and the anticipated consequences.
MNDB Scheme	Mandatory Notification of Data Breach Scheme, established in section 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (commenced 28 November 2023).
Personal Information	Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

8. Data Breach

A data breach occurs when personal information held by State Library is lost or subject to unauthorised access or unauthorised disclosure. A data breach can be accidental or intentional and may arise as a consequence of a cyber-attack, inadvertent disclosure, over-provisioning of access to sensitive systems or as a result of loss or theft of a physical device.

A data breach will be considered an 'eligible data breach' if the breach is likely to result in serious harm to affected individuals.

Serious harm occurs where the harm arising from the data breach has, or may, result in a real and substantial detrimental effect on an individual. Harm to an individual includes physical, economic, financial, social, emotional, psychological or reputational harm.

9. Reporting a data breach

Internal reporting

All actual or suspected data breaches that affect personal information must be reported immediately to the Compliance and Assurance Team.

Where the data breach is also an information security incident, the data breach must also be reported to the Service Desk or the Lead, Information Security.

External reporting

Members of the public can report a suspected data breach by contacting State Library using the email privacy@slq.qld.gv.au.

10. Responding to a data breach

State Library will follow a six-stage process to respond to data breaches. These stages are outlined in the Data Breach Response Plan. Specific responsibility for each of these Stages must be outlined in the Data Breach Response Plan

Stage 1: Preparation

1.1 Maintain an up-to-date Data Breach Response Plan. The Data Breach Response Plan must be reviewed annually by Compliance and Assurance and approved by the EDCS. The Data Breach Response Plan must also be reviewed by ELT in conjunction with the review of this Policy as per the Policy Review Schedule.

- Conduct regular training for employees on data breach prevention and response.
- Ensure robust security measures are in place, including encryption, access controls, and regular audits.

Stage 2: Identification

1.2 Identify and report suspected data breaches immediately to the Compliance and Assurance team. Information security incidents must also be referred to the Service Desk or the Lead, Information Security

- Conduct an initial assessment to determine whether a data breach has occurred.
- Document the details of the incident, including the date, time, and nature of the breach.

Stage 3: Containment and mitigation

- Take immediate steps to contain the breach and prevent further unauthorised access or disclosure.
- Implement measures to mitigate harm.

Stage 4: Assessment

- Assess the scope and impact of the breach, including:
  - the type of data involved
- the number of individuals affected, and
  - the potential for serious harm.
- Determine whether the breach meets the criteria for an **eligible data breach** under the IP Act and the Mandatory Notification of Data Breach (**MNDB**) scheme.

Stage 5: Notification

- If the breach is deemed to be an eligible data breach, EDCS (in consultation with ELT) is to notify the Office of the Information Commissioner Queensland (OIC) and affected individuals as soon as practicable.
- Notifications must include:
  - a description of the breach
  - the type of information involved
  - steps individuals can take to protect themselves
  - contact details for further information, and
  - if notification is not required, document the reasons for this decision.

Stage 6: Post data breach review and remediation

- Conduct a post-incident review to identify the root cause of the breach and evaluate the effectiveness of the response.
- Implement corrective actions to prevent future breaches, such as updating policies, improving security measures, or providing additional training.

11. Register of eligible data breaches

State Library will maintain an internal Register of Eligible Data Breaches, which will include:

- details of the breach (eg date, nature and scope)
- actions taken to contain and mitigate the breach
- assessment outcomes and notification decisions, and
- post-incident review findings and remediation actions.

State Library will review and update the Register on a regular basis.

12. Records management and privacy

State Library will document its management of, and response to, actual or suspected data breaches, in accordance with the Public Records Act 2023. Records will include evidence of compliance with this policy and relevant legislation.

Any records created in response to a data breach, including but not limited to tracking, reporting, assessing and determining eligible data breach status, management activities, communications and notifications must be managed in line with the Records Management Policy.

The privacy of affected individuals must be maintained in line with the Privacy Policy. Exemptions to specific privacy obligations may be applied in accordance with the MNDB Scheme.

13. Policy non-compliance and complaints

Non-compliance with this policy will be managed under the Code of Conduct and State Library Policies as appropriate.

Data breaches identified as part of a public interest disclosure must also be managed in line with the Public Interest Disclosures Policy.

Any complaints or privacy internal review requests arising from a data breach will be managed in line with the Privacy Policy.

14. References

This policy is supported by

Queensland Government

- Code of Conduct
- Queensland Procurement Policy
- Information Privacy Act 2009
- Information Privacy and Other Legislation Amendment Act 2023

State Library of Queensland

- Data Breach Response Plan
- Information Security Incident Response Plan
- Information Security Policy
- Procurement Policy
- Information Management Policy
- Privacy Principles Policy
- Payment Card Industry – Data Security Standards Compliance Policy
- Records Management Policy

15. Approval

18/11/2025

State Librarian and CEO

16. Creative Commons