Management of Personal Information Policy

File number:	635/380/006
Maintained by:	Director, Content Management
Review date:	April 2024
Next review date:	April 2027

1 Authority

State Librarian and CEO.

2 Responsibilities

State Library of Queensland has a responsibility to put measures in place to ensure the privacy and security of personal information collected.

Key roles and responsibilities:

State Library Officer/s	Activity
State Librarian and Chief Executive Officer	'Decision Maker' in relation to Right to Information Act 2009 (Qld) and Information Privacy Act 2009 (Qld), and responsible for the State Library's obligations under these acts.
Executive Director, Corporate Services	Internal 'Review Officer' in relation to Right to Information Act 2009 (Qld) and Information Privacy Act 2009 (Qld).
Manager, Compliance and Assurance	Responsible for the establishment and management of records management systems, policies and procedures to ensure effective information management and compliant recordkeeping.
Right to Information (RTI) and Privacy Officer	'Principal Officer' in relation to Right to Information Act 2009 (Qld) and Information Privacy Act 2009 (Qld).
Director, ICT Services	Director, ICT Services is responsible for technology requirements related to personal information security.
Executive Directors, Directors, Managers	Executive Directors, Directors, Managers are responsible for implementing the Policy in their business unit, and ensuring staff are aware of associated security processes, controls and mechanisms.

State Library Officer/s	Activity
Data stewards/owners	Data stewards/owners are accountable for creation, quality and retention/disposal of personal information in compliant systems in accordance with Information Management Policy.
All staff (permanent, casual or temporary)	All staff are responsible for making themselves aware of the requirements of the Policy and comply with State Library policies in accordance with Queensland Government Code of Conduct.
Clients	Clients are responsible for providing personal data that is accurate, complete, and up to date.

3 Policy statement

Personal information is a core business asset to State Library and is managed accordingly. The Management of Personal Information Policy (the Policy) provides guidance on how personal information is protected, managed, accessed, and shared.

4 Purpose

State Library collects personal information to provide access to collections and services, facilitate participation and collaboration, communicate with clients, as well as to meet business requirements and outcomes.

This Policy underpins the use and management of personal information collected from clients and supports the requirements identified in the Information Privacy Act 2009 which includes the *Information Privacy Principles (IPP)*.

The Policy provides high level guidance on how to manage personal information and balance the rights of individuals with legislative and contractual obligations.

The Policy provides a user-centric focus to service provision and interaction with State Library. This focus puts the client first by enabling personalised experiences and empowering clients to be open to discovery, participation and learning, and support the client's rights to privacy and access to their own personal information in State Library's possession.

The Policy also supports a standards-based approach to personal information management which enables implementation and compliance with technologies and methodologies.

The purpose of the Policy is to provide clients with information about how their personal information is protected, managed, accessed, and shared. Trust between State Library and its users is a key foundation for service delivery.

5 Scope

The Policy encompasses a whole of organisation approach to the collection of personal information for a range of purposes such as to access collections, membership registration, subscriptions to newsletters, attendance at events, programs, or training, requesting research, volunteering, or donations.

The Policy includes the management of personal information collected automatically or stored in other locations by companies based outside Australia and cloud-hosted services.

Personal information contained within State Library physical and digital collections are excluded from the Policy.

6 Definitions

Term	Definition
Anonymised data	The process of protecting private or sensitive information by erasing or encrypting identifiers that connect an individual to stored data or personal information.
Client	Members of the public who provide their personal information to State Library, includes both clients with, or without membership. State Library staff; permanent, casual or temporary who provide their personal information to State Library.
Data sharing	The process of making the same data available to multiple applications; including internal users and external companies and or vendors.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable. Personal information may include (noting the list is not exhaustive) name, address, date of birth, bank account number, IP address, equipment or software used or other highly sensitive information.

7 Principles

7.1 Privacy: Personal information is protected in accordance with the law

Rationale: State Library collects and stores personal information. Clients have a right to privacy and State Library is responsible for ensuring that such data is responsibly and transparently collected and managed.

This means:

- State Library complies with information privacy principles in the Information Privacy Act 2009, Information Privacy Principles and Information Management Policy
- Staff are educated and aware of compliance requirements in the Information Privacy Act 2009
- Staff act ethically and with integrity in accordance with the Queensland Public Service Code of Conduct, in particular clause 4.4 ensuring appropriate use and disclosure of official information
- Clients have a right to privacy, and to access and amend their own personal information in State Library's possession as per the Information Privacy Act 2009 and the Right to Information Act *(2009)*. Information on how clients can submit a request to access or update personal information can be found on the Information privacy and website security webpage
- Clients may request removal of their digital or print format from State Library managed records/data repositories as per the Right to Information Act *(2009)*. Clients may request the removal by contacting State Library.

7.2 Asset: Personal information is a core business asset to State Library of Queensland and is managed accordingly

Rationale: Personal information enables State Library to provide access to collections and deliver services, as well as meet business requirements and outcomes. Personal data is managed carefully to maximise its benefit to clients and the organisation.

This means:

- Staff are educated and aware of the value of personal information
- Staff with responsibility for systems which use, or access personal information have the authority and means to access and manage the data for which they are accountable
- Staff security roles and access permissions are audited regularly in accordance with the Information Security Policy
- Policy and procedures are used to ensure data quality, to reduce staff effort and waste and to enhance members' experiences
- Data stewards/owners are accountable for creation, quality and retention/disposal of personal information in compliant systems in accordance with Information Management Policy.

7.3 Trustworthy: Personal information is accurate, relevant, timely, accessible, and secure

Rationale: State Library collects the minimum level of data to provide access to collections and deliver services. Personal information is managed in an ethical and accountable manner throughout its lifecycle.

This means:

- Personal information is complete and captured 'right first time' in accordance with Information Privacy Principles (IPP 1-3)
- Personal information is relevant, collected for a purpose and to meet specific business requirements and outcomes, and will not be used for a purpose other than the particular purpose for which it was obtained, in accordance with Information Privacy Principles (IPP10)
- The minimum level of data required is collected to enable access to services and collections. State Library will only ask for the specific personal information required to fulfil the lawful purpose that is directly related to the functions of State Library, in accordance with Information Privacy Principles (IPP 1-3)
- Confidentiality, privacy, and security considerations underlie all decisions and are balanced against the right for the client to access their own personal information, in accordance with Right to Information Act 2009 and Information Privacy Principles (IPP 5-7)
- Personal information storage and security will be protected from loss, unauthorised access or misuse, in accordance with the Information Security Policy
- Personal information collected across State Library's physical, electronic and cloud-based environments is managed through its complete lifecycle; creation storage, use, sharing, archived and destroyed in accordance with the Public Records Act 2002 and the Information Management Policy.

7.4 Shared: Personal information is securely used and shared across State Library

Rationale: Timely access to personal information is essential to improve the quality and efficiency of both

members' and clients' experiences and staff's activities. Shared data will enable efficiency and cost savings and permit seamless identity access to all services.

This means:

- Staff have access only to the personal information necessary to perform their duties. Access permissions are audited regularly in accordance with the Information Security Policy.
- Personal information will not be used for a purpose other than the particular purpose for which it was obtained, in accordance with Information Privacy Principles (IPP10). However, alternate use is required under some circumstances
- Data may be shared within multiple applications for the purpose of providing access, analysis and delivering services
- Under no circumstances will the data sharing principle cause confidential information to be compromised
- To enable data sharing, a common set of procedures, standards and rules will be developed governing data management and access in accordance with the Information Management Policy. This includes consistent language used in data field labels
- Personal information collected automatically i.e. IP addresses, or stored in other locations by companies based outside Australia and cloud-hosted services are only allowed to use the data for contractually agreed purposes and must handle data in a confidential and secure manner in accordance with Queensland privacy legislation Information Privacy Act 2009 and Information Privacy Principles (IPP 1-3)
- Duplication of data and redundant effort is minimised
- Anonymised data will be used in open data initiatives and reporting activities
- Anonymised data will be used to enable authentication with external service providers in a federated identity environment.

8 Essential considerations

Review of the Policy has included considerations of the 23 fundamental human rights protected under the *Human Rights Act 2019*. When applying the Policy, the State Library will act and make decisions in a way that is compatible with human rights and give proper consideration to all human rights, as required by the *Human Rights Act 2019*.

The *Human Rights Act 2019* exists to:

- Protect and promote human rights
- Help build a culture in the Queensland public sector that respects and promotes human rights
- Help promote a dialogue about the nature, meaning and scope of human rights.

The *Human Rights Act 2019* protects 23 fundamental human rights drawn from international human rights law, including the following rights:

- Freedom of thought, conscience, religion and belief
- Freedom of expression
- Taking part in public life
- Privacy and reputation
- Protection of families and children
- Cultural rights – generally
- Cultural rights – Aboriginal peoples and Torres Strait Islander peoples

- Right to liberty and security of person.

9 Risk management and mitigation

Risk	Description of risk	Mitigation management
Personal information breach	Failure to enforce information security, including cyber security and client personal information, resulting in inability to deliver services, loss of reputation and trust or exposure to security breaches.	The current State Library Risk Profile is available on the intranet. It outlines risks and treatment strategies to mitigate risks for State Library. The Audit and Risk Management Committee (ARMC) oversees risk management. The Risk Profile is reviewed annually by the ARMC and the Library Board. 2022-23 State Library risk profile.
Personal information breach	Breach or misuse of confidential information by staff.	Mandatory training to reinforce the importance of policies and guidelines. Regular audit of staff permissions and access to identity management systems.
Security compliance	As there are many areas across State Library collecting, storing and using personal information, there is a risk to the organisation if they are not compliant with the principles and requirements of this policy.	Mandatory training Review of procedures to ensure compliance with the Policy. Review of security compliance where information is collected automatically or stored in other locations by companies based outside Australia and cloud-hosted services.
Removal of digital or print format	Failure to remove client details from all business applications or software.	Training provided in Identity Management Policy and adherence to procedures and processes.

10 References

The policy is supported by:

Queensland Government

- Electronic Transactions Act 2001
- General Retention and Disposal Schedule (GRDS)
- Human Rights Act 2019
- Information Privacy Act 2009
- Information Privacy Principles
- Information Standard IS18 – Information Security
- Public Records Act 2002
- Public Sector Ethics Act 1994
- Right to Information Act 2009
- Right to Information Act 2009 (the RTI Act)

- Queensland Government Information security classification framework (QGISCF)
- Queensland Public service Code of Conduct
- Queensland State Archives Records Governance Policy.

State Library of Queensland

- Information Security Policy
- Information Management Policy
- Information privacy and website security
- Protective Security Policy
- Your Information Guidelines.

11 Approval

Approved by State Librarian and CEO 20 May 2024.

12 Creative Commons