



Identity Management principles

Policy Number:	CD-CA-001-V01
Records File Number:	695-165-004
Maintained By:	Collection Access
Review Date	2016

1. Document Control

Version	Approved By	Approval Date	Revisions
1	Executive Team	28/2/14	

2. Purpose

State Library of Queensland collects data to enable access to our collections and services. The principles in this document underpin the use and management of identity data at State Library of Queensland. These principles foster a whole of organisation approach to identity management and provide high level guidance to manage our data assets and to balance the rights of individuals with legislative and contractual obligations.

These principles provide a user-centric focus to service provision. This focus puts the client first by reducing barriers to registration, authentication and access, enabling personalised experiences and empowering clients to self-manage their personal information and needs regardless of how and where they access State Library.

The principles also support a standards based approach to identity management which will enable implementation of new and existing technologies and methodologies, such as Open ID and Security Assertion Markup Language (SAML).

3. Policy Statement

1) **Asset: Identity data is a core business asset to State Library of Queensland and is managed accordingly**

Rationale: Identity data enables State Library of Queensland to provide access to collections, services and facilities and to communicate with our members. SLQ carefully manages data to maximise its benefit to members and the organisation.

Implications:

- Staff are educated and aware of the value of identity data.

- Staff with responsibility for systems which use or access identity data have the authority and means to access and manage the data for which they are accountable.
- Policy and procedures are used to ensure data quality, to reduce staff effort and waste and to enhance members' experiences.
- Data stewards/owners are identified at the Executive Manager level and are accountable for creation, quality and retention/disposal of identity data in compliant systems.

2) Trustworthy: Identity data is accurate, relevant, timely, accessible and secure

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

Implications:

- Identity data is complete and captured "right first time".
- Identity data is relevant, collected for a purpose and to meet specific business requirements and outcomes.
- The minimum level of data required is collected to enable access to services and collections.
- Identity data is managed through its complete lifecycle from registration, activation, maintenance, deactivation and deletion.
- Confidentiality, privacy and security considerations underlie all decisions and are balanced against the right to information.
- State Library maintains a central authoritative store for identity data but copies of data may be stored in other locations as required including cloud-hosted services.
- Retention and disposal of identity data is managed appropriately and in a timely manner.

3) Shared: Identity data is securely shared across State Library of Queensland and derived from a single authoritative source

Rationale: Timely access to identity data is essential to improve the quality and efficiency of both members' experiences and staff's activities. Shared data will enable efficiency and cost savings and permit seamless identity access to all State Library of Queensland services.

Implications:

- State Library of Queensland maintains a central authoritative store for identity data but copies of data may be stored in other locations as required including in cloud-hosted services.
- Members need register only once to access to collections and services. Permission and privilege levels are identified through agreed processes to enable streamlined easy access to SLQ services.
- Staff have access to the identity data necessary to perform their duties.
- To enable data sharing, a common set of procedures, standards and rules will be developed governing data management and access. This includes consistent language used in data field labels.
- Duplication of data and redundant effort is minimised.
- As legacy systems are replaced, new applications and systems must be compliant with the shared environment.
- Under no circumstances will the data sharing principle cause confidential information to be compromised.
- Anonymized data will be used in Open Data initiatives and reporting activities.

- Anonymized data will be used to enable authentication with external service providers in a federated identity environment, such as Eduroam.

4) Private: Personal information is protected in accordance with the law

Rationale: State Library of Queensland collects and holds personal information about its members. Individuals have a right to privacy and State Library is responsible for ensuring that such data is responsibly and transparently collected and managed.

Implications:

- State Library of Queensland complies with information privacy principles in the *Information Privacy Act 2009*.
- Once registered members will be empowered to access and amend their own personal details online.
- Staff are educated and aware of compliance requirements in relation to privacy.
- Staff act ethically and with integrity in accordance with the *Code of Conduct for the Public Service*.
- Individuals 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*).

4. References

The Policy is supported by:

- *Information Privacy Act 2009*
- *Right to Information Act 2009*
- *Code of Conduct for Public Service*

5. Approval date

Approved by the Executive Team, February 28 2014.