Data Management - Procedures

Definitions

Please refer to the University's Glossary of Terms for policies and procedures. Terms and definitions identified below are specific to these procedures and are critical to its effectiveness:

Corporate data: Data is the representation of facts as text, numbers, graphics, images, sound or video. Corporate data is data that is captured through the operation of the University. It can include, but is not restricted to: staff data, student data, financial data, facilities data, curriculum data, etc.

Personal data: Personal data is data where a person's identity is apparent, or can reasonably be ascertained. Note that a person's name is not necessary for data to be personal.

Master data: Master data is data about the business entities that provide context for business transactions. It is the authoritative and most accurate data available and is used to establish the context for corporate data.

Reference data: Reference data is used to classify or categorise other data. It can include, but is not restricted to, status codes, state abbreviations, demographic fields, etc.

1. Purpose of procedures

These procedures provide guidance and direction on the management of corporate data throughout the information lifecycle.

2. Scope and application

These procedures apply to University corporate data in all formats. These procedures are further supported by guidelines and other local documents as identified.

Research data procedures aligning with the Australian Code for the Responsible Conduct of Research are available via the Research Data and Materials – Procedures under the overarching Research – Academic Policy.

3. Data governance

University corporate data management activities exist to effectively and efficiently manage the data assets of the University. With a focus on continuous improvement, the Data Management Group (staff login required) contributes to decisions on the collection and management of data, proactively defines data rules, resolves data issues, and fosters an organisational approach to data handling. Minutes from Data Management Group meetings are available on MyUniSC (staff login required).

4. Data management

4.1 Corporate data should be collected only when known and documented uses and value exist.

4.2 Collection of accurate and complete data is expected, even when elements are required by a cost centre of the University which is different to the cost centre undertaking the collection.

4.3 The University collects and uses personal data about its students, staff and others in order to operate effectively. Personal data held by the University is collected and managed in a responsible, secure manner, in compliance with the Information Privacy Principles outlined in the *Information Privacy Act 2009* (Qld). Guidance on Information Privacy is covered in the Information and Records Management – Procedures. Access to personal data within the University is restricted to authorised staff with business process requirement. See 'Personal information – Guidelines' on MyUniSC (staff login required).

4.4 For accountability and stewardship, all data must have a defined Data Steward responsible for accuracy, integrity, and security of data. Data Stewards are responsible for ensuring that all legal, regulatory, and policy requirements are met in relation to specific data assets. A list of Data Stewards is available on MyUniSC (staff login required).

APPROVAL AUTHORITY

Vice-Chancellor and President

RESPONSIBLE EXECUTIVE MEMBER

Vice-Chancellor and President

DESIGNATED OFFICER

Head, Information Governance

FIRST APPROVED

5 June 2017

LAST AMENDED

8 June 2017

REVIEW DATE

7 June 2022

STATUS

Active

4.5 Endorsed systems for the storage of corporate data are listed in the Information and Communication Technology (ICT) Security - Operational Policy, Schedule A – Business Systems. Where practical, data should be recorded in an auditable and traceable manner.

4.6 Whilst data re-use is encouraged, data duplication is discouraged. For integrity, data should be entered only once, and any duplication of the collection or storage of data needs approval of the relevant Data Steward and reported to the Data Management Group. Staff should collaborate to prevent the storage of duplicate data assets, wherever possible referring to an organisational single source of truth rather than saving a local copy.

4.7 The timely destruction of data is essential for effective management. Corporate records are destroyed after fulfilling the minimum retention period prescribed in records authorities issued by Queensland State Archives. Retention periods in records authorities consider business, legal and government requirements and the University uses several general and agency-specific authorities to determine retention, destruction and transfer actions for its records.

4.8 Processes for data capture, validation and processing should be automated wherever possible.

4.9 Business processes must ensure the maintenance of reliable data. All corporate data management practices in the University are to be in accordance with these procedures and related policy.

4.10 Data management resources for staff are available on MyUniSC (staff login required). Data Stewards are responsible for identifying training requirements for their data domain/s and ensuring appropriate training is in place.

5. Master data management

The UniSC Data Hub, under the management of Information Technology (IT), supports master data services for the organisation. Commonly-used corporate data is held within the Data Hub based on rules provided by the Data Stewards to ensure consistency and integrity. The Data Hub data is distributed to various systems upon agreement with the Data Stewards regarding usage.

6. Data domains

Information systems may operate across multiple data domains and, where necessary, multiple Data Stewards may be required to work collaboratively on data in a single system. The University has adopted the CAUDIT Data Reference Model which defines the agreed terminology and key concepts important to the business. The model can be used to identify where data is stored, who is responsible for governing the data, and data quality risks. The data reference model is available on MyUniSC (staff login required).

7. Data quality

A collaborative approach for addressing enterprise data quality issues is critical to maintaining data integrity. Data quality issues relating to: accuracy, completeness, duplication and/or currency of data, or changes to business processes impacting on data collection and recording, should be provided to the Data Management Group and the issue recorded in the Data Quality Register. It will then be assigned to the appropriate Data Steward who will conduct: preliminary/root cause investigation, evaluation of possible solutions, and a proposed solution. The Data Steward may call on Data Administrators and other members of the University community to assist in this step. Outcomes will be presented at the next Data Management Group meeting and escalated, where required, to the Information Management Committee. The Data Steward is responsible for the implementation of a solution to resolve the data quality issue.

At times, an identified data quality issue will be outside the responsibilities of the assigned Data Steward. In these instances, it may take further resources to identify the root cause and propose a solution.

8. Data accessibility

The University, rather than any individual or cost centre, owns corporate data. A culture of data sharing is encouraged and data must be readily available to staff with a legitimate business need. Data is a corporate asset to which all staff should have access to do their jobs, except where the nature of the data requires restriction.

9. Data security

Data must be protected from unauthorised access and modification. For information asset security classification and related handling requirements, see 'Information asset security classifications and handling – Guidelines' on MyUniSC (staff login required). For further information on organisational information technology security, see ICT Security - Operational Policy.

10. Roles and responsibilities

Assigning responsibilities to data management ensures data is appropriately identified and managed throughout its lifecycle and is accessible to appropriate stakeholders. The University adopts a federated model for data accountability, with a focus on data stewardship, and not data ownership.

	ROLE	RESPONSIBILITIES	APPOINTED BY
Data Governance	Information Management Committee	Providing leadership, direction and strategic advice on the planning and delivery of information management best practice in alignment with USC's Strategic Plan.	ICT Governance Committee
Data Management	Data Management Group	Convene to make decisions about the treatment of data assets.	Information Management Committee
Data Steward*	For accountability and stewardship, all data must have a defined Data Steward responsible for accuracy, integrity, and security of data. Data management, authority and accountability for data assets within their allocated data domain. This includes ensuring: Data value to the organisation is fully realised. Data is shared to the maximum extent possible in accordance with security requirements. Data quality is actively maintained to a high standard. Business process for the data is established. Concerns of others relating to data assets under their care are addressed.	Information Management Committee	
Data Administrator*	Administration of data assets, as directed by the relevant Data Steward. This includes: Understanding the business process, value, security level, and risks of the data set. Monitoring data quality.	Data Steward	
Data User	Adherence to policies, procedures and guidelines to ensure data quality and security is maintained.		

* The list of Data Stewards and Data Administrators can be found on MyUniSC (staff login required).

END

RELATED DOCUMENTS

- Information Management Framework - Governing Policy

LINKED DOCUMENTS

- Information Management Framework - Governing Policy

RELATED LEGISLATION / STANDARDS

- Right to Information Act 2009 (Qld)
- Public Records Act 2002 (Qld)
- Queensland Information Standards
- Information Privacy Act 2009 (Qld)