Data Management - Procedures

1. Purpose

1.1 These procedures operationalise the apporach for managing University data and information throughout the data lifecycle and the use of data models.

1.2 These procedures must be read in conjunction with the linked Data Governance – Operational Policy, Privacy and Right to Information - Operational Policy, Privacy Management - Procedures, Right to Information - Procedures, Data Classification - Procedures, Records Management – Procedures, and Data Handling – Guidelines (login required).

2. Scope and application

2.1 These procedures apply to all University staff, students undertaking research or involved in other University business, approved third parties, alumni, contractors, and sub-contractors. It includes all individuals who handle University data and information, regardless of their role or affiliation.

2.2 These procedures apply to all University data and information.

3. Definitions

3.1 Refer to the University's Glossary of Terms for definitions as they specifically relate to policy documents.

3.2 The terms data and information are used interchangeably within this policy, recognising the overlap between the two. In their simplest form, data is often considered as raw values and individual facts in any form, and information is data that has been contextualised. Both data and information can be University records.

APPROVAL AUTHORITY

Chief Operating Officer

RESPONSIBLE EXECUTIVE MEMBER

Chief Operating Officer

DESIGNATED OFFICER

Chief Data Officer

FIRST APPROVED

5 June 2017

LAST AMENDED

3 December 2024

REVIEW DATE

3 December 2026

STATUS

Active

4. Data lifecycle management

4.1 At each stage of the data lifecycle (as depicted in Figure 1: Data lifecycle), data management enscaputales the key elements of compliance, security, privacy, integrity, ethical considerations, training, literacy, and accountability in accordance with the Data Governance – Operational Policy.

Figure 1: Data lifecycle

4.2 Capture

4.2.1 All University data and information must be captured in an approved business system (login required).

4.2.2 When capturing data or information, attention must be given to assuring accuracy, reliability, consistency, and completeness at the point of data entry.

4.2.3 Responsible and compliant collection of personal information must adhere to the Privacy and Right to Information - Operational Policy and Privacy Management - Procedures.

4.2.4 Where practicable (i.e. based on business system capability), data must be classified at the point of capture, in accordance with the Data Classification - Procedures, and guidance from the Data Custodian.

4.3 Store

4.3.1 Appropriate security and access controls should be applied for the storage of data, based on data classification in accordance with Data Classification - Procedures, intended audience, privacy, confidentiality, and business needs. Security and access controls can be digital (e.g. controls within a business system) or physical (e.g. swipe card access), depending on the format of the data.

4.3.2 The location and jurisdiction of services used for the storage of data – partcularly personal information – must be considered in accordance with the Privacy and Right to Information - Operational Policy, Privacy Management - Procedures, ICT Security - Operational Policy, and Adopting Cloud-based Services - Procedures. This includes the consideration of the location of data servers and country of operation for cloud-based services.

4.3.3 Storage of personal information within Australia is the University's preferred approach. When personal information is stored outside Australia, this must comply with the requirements under the Privacy Management - Procedures and *Information Privacy Act 2009 (Qld)*.

4.4 Utilise

4.4.1 The use of data and information must be for approved business purposes, in alignment with the University's values and mission. All Data Users are responsible for ensuring their use of data is responsible, ethical and compliant with University policy documents, and legislative obligations.

4.4.2 Read and write controls for data must be appropriately managed based on business need, to ensure accuracy, quality and integrity is maintained and align with data classification in accordance with the Data Classification - Procedures.

4.4.3 Personal information must only be used for permitted purposes in accordance the Privacy Management - Procedures.

4.4.4 Data Users must ensure data is of sufficient quality for their proposed use, to ensure the verracity of outputs generated and reliability for data-driven decision-making. Data Custodians are responsible for the oversight of data quality within their data domain.

4.4.5 Data changes must be approved by the Data Change Advisory Board (Data CAB). The Data CAB is responsible for considering impacts to enterprise architecture, business systems, processes, and stakeholders. Further information about data change requests is available on the Data Portal (login required).

4.5 Share

4.5.1 Sharing of data and information beyond its original intended audience, in accordance with access controls applied at Store stage, requires approval in writing from the relevant Data Custodian. This includes sharing internally (e.g. between Departments) and external to the University.

4.5.2 Any sharing of personal information must be in accordance with the Privacy Management - Procedures.

4.5.3 Security of data in transit must be considered in accordance with the ICT Security - Operational Policy and Data Classification - Procedures, based on the privacy, confidentiality and classification of the data.

4.6 Archive

4.6.1 Data and information identified as University records must be archived in accordance with the Records Management – Procedures.

4.7 Dispose

4.7.1 University data and information must only be disposed of once there is no longer an active business, legal or compliance requirement for retention. Data Custodians are responsible for oversight for the destruction of data within their data domain.

4.7.2 Disposal of University records must be in accordance with the Records Management – Procedures and Disposal of Records – Guidelines (login required).

4.7.3 Disposal of data must utilise secure and irreversible methods to ensure data is permanently eradicated or de-identified beyond recovery.

5. Data model: data domains, subdomains, and assets

5.1 This section details the University's approach to managing data domains, subdomains, and assets, ensuring strategic governance across its data model (as depicted in Figure 2: Data domains).

Figure 2: Data domains

5.2 Data domains

5.2.1 Data domains are conceptual groupings of data by business context, concept or other high-level commonality.

5.2.2 Data domains are assigned a Data Custodian who is responsible for the overall management of data in that domain. The Chief Data Officer is responsible for appointing a Data Custodian for each data domain defined within the University.

5.2.3 Data Custodians are responsible for the data assets within their data domain, ensuring management throughout the data lifecycle.

5.3 Data subdomains

5.3.1 Within each data domain is a number of data sub-domains. Data sub-domains provide a more specific means of grouping similar data assets to improve discoverability and enable the practical management of data assets throughout the data lifecycle.

5.4 Data assets

5.4.1 At the most granular level are data assets. Data assets can include University documents, data tables within business systems, web pages, learning materials, physical files and records, video and audio recordings, or assessment materials.

6. Research data management

6.1 In specific situations, additional or alternate data management practices and controls can apply to data and information relevant to research management activities or projects. Research data must be managed in accordance with the Research Data Management - Procedures and Responsible Research Conduct - Academic Policy.

7. Monitoring and reporting

7.1 Regular monitoring and reporting on the application of the Data Management – Procedures is reported the Data Analytics and Information Management Advisory Committee.

7.2 The Chief Data Officer monitors and reports on University compliance with these procedures in accordance with the Compliance Management Framework - Governing Policy.

8. Authorities and responsibilities

8.1 As the Approval Authority the Chief Operating Officer approves these procedures to operationalise the Data Governance – Operational Policy.

8.2 As the Designated Officer of these procedures the Chief Data Officer is authorised to approve associated documents to support the application of these procedures.

8.3 These procedures operate from the last amended date, with all previous procedures related to data management replaced and having no further operation from this date.

8.4 All records relating to data management must be stored and managed in accordance with Records Management – Procedures.

8.5 These procedures must be maintained in accordance with the Policy Framework - Procedures and reviewed on the shortened 2-year policy review cycle.

8.6 Any exception to this policy to enable a more appropriate result must be approved in accordance with the Policy Framework - Procedures prior to any deviation from these procedures.

8.7 Refer to Schedule C of the Delegations Manualin relation to the approved delegations detailed within these procedures.

8.8 Data management roles

8.8.1 The following roles, responsibilities and accountabilities are specific to this procedure and cascade from the high-level roles and responsibilities in the Data Governance – Operational Policy.

ROLE	POSITION	RESPONSIBILITY AND ACCOUNTABILITY
Data Champion	Vice Chancellor and President	Accountable for: (a) championing the University's data management practices.
Chief Data Officer	Chief Data Officer	Accountable for: (a) risk assurance for data management related risks. Responsible for: (a) implementing procedures, supporting guidance, and uplifting data literacy across the University to promote compliant and responsible data management practices; (b) appointing and inducting Data Custodians for each Data Domain and ensuring their awareness of data management responsibilities; (c) administrative management of the Data Change process and Data Change Advisory Board; and

		(d) monitoring and reporting on adherence with these procedures.
Data Custodian	Heads of Departments (appointed by CDO)	Responsible for: (within their data domain) (a) providing guidance on the classification of data; (b) approval of data sharing requests; (c) advising on potential impacts associated with data change requests; and (d) providing oversight for data quality.
Data Subject Matter Experts	Staff based on specific expertise-criteria relative to a data asset	Responsible for: (a) providing expert advice on business or technical matters related to specific data assets; and (b) supporting governance processes and decisions, including those related to data access, sharing, and changes.
Business System Owner	In accordance with the ICT Security - Operational Policy	Responsible for: (a) ensuring business systems are secure to protect data throughout its lifecycle; (b) implementing classification labelling functionality within their system, where applicable; and (c) monitoring and reviewing the application of technical system controls to secure data and control access throughout its lifecycle.
Data User	All University staff and/or groups that create and use data	Responsible for: (a) using data in a responsible, ethical and compliant manner, for an approved business purpose; and (b) adhering to all policy document requirements.

END

RELATED DOCUMENTS

- Acceptable Use of ICT Resources - Operational Policy

- Adopting Cloud-based Services - Procedures
- Compliance Management Framework - Governing Policy
- Compliance Management Framework - Procedures
- Critical Incident Management - Operational Policy
- Data Breach - Procedures
- ICT Security - Operational Policy
- Incident Management - Procedures
- Research Data Management - Procedures
- Responsible Research Conduct - Academic Policy
- Risk Management - Governing Policy
- University Policy Documents - Procedures

LINKED DOCUMENTS

- Data Classification - Procedures

- Data Governance - Operational Policy
- Privacy and Right to Information - Operational Policy
- Privacy Management - Procedures
- Records Management - Procedures
- Right to Information - Procedures

RELATED LEGISLATION / STANDARDS

- Right to Information Act 2009 (Qld)
- Public Records Act 2023 (Qld)
- Privacy Act 1988 (Cth)
- Spam Act 2003 (Cth)
- Information Privacy Act 2009 (Qld)
- Invasion of Privacy Act 1971 (Qld)
- General Data Protection Legislation (EU/UK)