Data Governance - Operational Policy

1. Purpose

1.1 This policy outlines the University's unified approach for data governance, underpinning how the University collects, creates, manages and uses data and information in a secure, compliant, and consistent manner.

1.2 Understanding what data, the University holds, where it is located, how it needs to be managed and the distributed responsibility for its management, are core elements of data governance. Implementing a formal approach to data governance improves data quality and integrity, facilitate data governance controls through dedicated roles and responsibilities and enable better informed operations, decision-making and strategic planning.

1.3 This policy must be read in conjunction with the linked Data Classification - Procedures, Records Management – Procedures, Data Management - Procedures, and Data Breach - Procedures.

2. Scope and application

2.1 This policy applies 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 This policy applies 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.

4. Policy statement

4.1 The University recognises data governance as the foundation of effective data management, which underpins evidence-based decision making and compliance with privacy and data protection legislation. Embedding a strong data governance foundation across the University improves data quality and integrity, promotes data trust and improves realisation of value from the University's data as a strategic asset. The implementation of a consistent data governance approach with distribution of responsibility for decision rights across the University, assures accountability for how data is managed and used, promotes best practice in data protection and aligns with compliance requirements and responsible practice.

5. Principles

5.1 The University has adopted 6 data governance principles to inform behaviour when creating and using data in University operations.

5.2 Accountability for data through its lifecycle is everyone's responsibility.

5.2.1 The University is committed to an effectively governed data ecosystem, which at its core ensures everyone plays a key role in managing data. All data users are accountable for how they handle data through the stages of the data lifecycle. Adherence to legislative obligations, policies, procedures, and processes by all data users is essential to ensure University data is of a high quality and managed with integrity, in an efficient, compliant, secure, and responsible way.

5.3 Creating and maintaining quality data by all data users, is fundamental to building data trust and enabling realisation of data value.

5.3.1 The University expects all users to commit to an ethos of creating, maintaining, and delivering quality data, that is accurate, reliable, consistent, complete, timely and meaningful. This ensures data can be trusted to inform decision-making, improve organisational efficiency, meet compliance requirements, and support the University's strategic objectives. The University is committed to a program of continuous innovation and improvement in data management, that will enable optimum data quality.

APPROVAL AUTHORITY

Vice-Chancellor and President

RESPONSIBLE EXECUTIVE MEMBER

Chief Operating Officer

DESIGNATED OFFICER

Council Secretary

FIRST APPROVED

22 September 2015

LAST AMENDED

3 December 2024

REVIEW DATE

3 December 2029

STATUS

Active

5.4 Cultivating data literacy in the University workforce is critical to effective data utilisation.

5.4.1 The University is committed to building a highly data-literate workforce through a program of continuous training and support for all University data users, that enhances understanding of the scope and potential of the University's data and builds capability in responsible practice for data handling and use. A highly data literate University workforce will drive agility, knowledge, and productivity and enable optimum data utilisation, both operationally and strategically.

5.5 Data must be discoverable to facilitate access and collaborative use.

5.5.1 Ensuring data is discoverable within all aspects of University operations, will ensure data users can find, access, and utilise the data they require, balancing openness with confidentiality, privacy, and security requirements. This approach promotes interdisciplinary collaboration and innovation within University data users and drives overall efficiency in the use of data.

5.6 Data is protected by everyone to safeguard confidentiality, integrity, privacy and continuity.

5.6.1 Protection of data is the collective responsibility of everyone in the University. Robust access and security controls, established processes and responsible practice, prevent unauthorised access, interference, disclosure, or loss and assures compliance and integrity in every data interaction.

5.7 Using data ethically is imperative to recognise and embrace equity, diversity and inclusion and reflect community values.

5.7.1 An ethical approach to data use is essential for ensuring that University practices not only meet community expectations, but also respect individual rights and dignity in a rapidly evolving digital landscape. Positioning ethics at the core of the University's data usage commits not just to equity, diversity, and inclusion, but also to a proactive engagement with the ethical complexities that emerge. This approach ensures the University's actions, benefit society and protect the privacy and rights of individuals involved.

6. Data lifecycle

6.1 The data lifecycle reflects how data and information moves through various stages of use, and aims to ensure data and information is managed responsibly at all times.

6.2 Across all stages of the data lifecycle, the University upholds a commitment to continuous oversight, review, and improvement. Proactive planning and thoughtful design are embedded in each stage, shaping the journey of data from its inception to its final disposal if appropriate. This approach enables the confidentiality, integrity, availability, security, and quality of University data and information.

6.3 There are 6 stages to the University's data lifecycle, as shown in Figure 1: Data lifecycle. Mostly, data and information follow a sequential order from capture to disposal, although at times it is not strictly linear, and some stages may not be relevant for certain types of data or information.

Figure 1: Data lifecycle

6.4 Capture

6.4.1 This stage involves, the creation (generation of new content) or acquisition (intake of existing content) of data or information within the University data ecosystem. Acquisition of data can also include data collection via automated systems or processes.

6.4.2 Controls must be implemented to ensure data is complete, reliable, accurate, timely and responsibly captured to ensure data quality and integrity.

6.5 Store

6.5.1 This stage involves managing and maintaining data in appropriate locations, including University approved business systems and physical storage. Applying access and technical controls in accordance with Data Classification - Procedures, along with capturing meta-data and implementing security measures, is key to ensuring data's confidentiality, integrity, quality, availability and protection. Storing data should also be undertaken in accordance with the Records Management – Procedures and Data Handling – Guidelines (login required).

6.6 Utilise

6.6.1 This stage includes the performance of actions including data transformation, manipulation, analysis, or other processing, undertaken to extract value, support business processes and generate insights. Ensuring ethical and compliant data use, including protecting the privacy of individuals, is of uppermost importance. Promoting interdisciplinary collaboration for greater accessibility and innovation is encouraged, considering applicability based on confidentiality and permitted use.

6.7 Share

6.7.1 This stage includes a focus on ensuring secure and appropriate practice when data is shared, accessed, or retrieved, using relevant processes and controls by persons or systems. The University promotes an open and transparent approach to data sharing where appropriate, that enables cross-unit collaboration.

6.7.2 When sharing data externally, consideration must be given to determine the appropriateness of the data for external access and use, along with the necessary controls to enforce compliance, ensure confidentiality and data security, and protect privacy in accordance with the *Information Privacy Act 2009 (Qld)* and *Right to Information Act 2009 (Qld)*. Unauthorised or accidental sharing or disclosure should be managed in accordance with the Data Breach - Procedures.

6.8 Archive

6.8.1 This stage includes a focus on when data or information is no longer in active use. This involves the longer-term preservation of data or information to support University business, meet requirements for University records under the *Public Records Act 2023 (Qld)* or otherwise as required by law, or because the information has historical or cultural value.

6.8.2 University records must be captured in the approved record keeping system, in accordance with the Records Management – Procedures.

6.9 Dispose

6.9.1 This stage includes a focus on the processes and methods for the secure disposal or destruction of data, in digital or physical form. This phase also includes transferring data control to another entity. Adherence with legislative requirements is essential when data – including University records – are disposed in accordance with the Records Management – Procedures.

7. Data model

7.1 This section must be read in conjunction with Section 5 - Data model: data domains, subdomains, and assets of the Data Management - Procedures which details the University's process for application of a data model.

7.2 The University's data model underpins the identification and definition of data domains, subdomains, and assets, and is based on the CAUDIT Higher Education Data Reference Model.

7.3 The organisation of data at the University utilises a hierarchical approach and enables a clear assignment of roles and responsibilities for management of the University's data a documented in Figure 2: Data domains.

Figure 2: Data domains

7.4 The University organises data into data domains, are logical groupings of data by purpose, concept or other commonality. Each high-level data domain contains one or more data subdomains, which is a category of data, which enables more definitive management. Within data subdomains are data assets, which represent documents, databases, web pages or other groupings of data that have a relationship to the data subdomain.

8. Data governance roles and decision making

8.1 Roles, responsibilities and accountabilities

8.1.1 The assignment of data governance roles with their associated accountabilities and responsibilities are fundamental for successful governance of University data. Formally appointed roles include the Data Custodians. All University staff are considered data users.

ROLE	POSITION	RESPONSIBILITY AND ACCOUNTABILITY
Data Champion	Vice-Chancellor and President	Accountable for: (a) delegating powers for data compliance obligations under legislation; and (b) champions a data-driven culture, underpinned by effective governance that supports the University's strategic direction.
Chief Data Officer	Chief Data Officer	Delegated officer for legislative powers and functions under the *Right to Information Act 2009 (Qld)*, the *Information Privacy Act 2009 (Qld)* and the *Public Records Act 2023 (Qld)*. Accountable for:

		(a) ensuring data governance processes and practices are embedded across the University; (b) assurance for data-related risks; and (c) conformity with this policy and related procedures. Responsible for: (a) implementation, oversight, and advocacy for the University's data governance approach and related initiatives; (b) promoting the University's data and information policy documents; (c) monitoring compliance with legislation, policies and procedures; (d) appointing data custodians and induction of appointed individuals; (e) regular reporting to data and information committees on data governance adoption, practices and compliance; (f) providing direction for identification and management of data-related risks; (g) incorporating data governance responsibilities within relevant University governing committees with appropriate decision-making powers; and (h) implementation of the Data & Analytics Operating Model that defines data domains and sub-domains and its associated decision rights responsibilities.
Data Custodians	Heads of Departments (as appointed by the CDO)	Responsible for: (within their data domain) (a) establishing and maintaining local processes and practices for whole-of-lifecycle management of data. (b) identification and management of data-related risks; (c) promoting and remediating data quality; (d) championing ethical data use; (e) approval of data access, sharing and change requests; and (f) identification of Data Subject Matter Experts to support governance processes and operational decisions related to data.
Business System Owners	In accordance with the ICT Security - Operational Policy	Responsible for: (a) implementing and reviewing technical controls, including for security and access, to protect and maintain data assets stored in University approved business systems throughout their lifecycle; and (b) regular engagement with Data Custodian to align expectations for the management of data in their data domain within systems.
Data Subject Matter Experts	Staff based on specific expertise-criteria relative to a data asset	Responsible for: (a) providing expertise for business or technical matters relating to specific data assets; and (b) providing context and support for data processes and decisions, including access, sharing and change requests.
Data Users	All University staff or affiliates that create and use University data	Responsible for: (a) working with data in a compliant and responsible way in accordance with legislation and the requirements of University policy documents.

8.2 Decision rights

8.2.1 The decision rights model demonstrates the hierarchical relationship between data governance roles and their associated responsibilities, providing a clear framework to support data governance decision-making.

Figure 3: Decision rights model

9. Reporting and Monitoring

9.1 Regular monitoring and reporting on the application of data governance policy and underpinning procedures, is reported by the Chief Data Officer on a quarterly basis to the Data Analytics and Information Management Advisory Committee.

9.2 The Chief Data Officer monitors and reports on University compliance with this policy in accordance with the Compliance Management Framework - Governing Policy.

10. Authorities and responsibilities

10.1 As the Approval Authority, the Vice-Chancellor and President approves this policy in accordance with the *University of the Sunshine Coast Act 1998 (Qld)*.

10.2 As the Responsible Executive Member the Chief Operating Officer can approve procedures and guidelines to operationalise this policy. All procedures and guidelines must be compatible with the provisions of this policy.

10.3 As the Designated Officer the Chief Data Officer can approve associated documents to support the application of this policy. All associated documents must be compatible with the provisions of the policy.

10.4 This policy operates from the last amended date, all previous iterations of policies related to data governance are replaced and have no further operation from this date.

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

10.6 This policy must be maintained in accordance with the Policy Framework - Procedures and reviewed on the standard 5-year policy review cycle.

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

10.8 Refer to Schedule C in the Delegations Manual in relation to the approved delegations detailed within this policy.

END

RELATED DOCUMENTS

- Acceptable Use of ICT Resources - Operational Policy

- Acceptable Use of ICT Resources - Procedures
- Compliance Management Framework - Governing Policy
- Compliance Management Framework - Procedures
- Critical Incident Management - Operational Policy
- ICT Access Control - Operational Policy
- ICT Security - Operational Policy
- Incident Management - Procedures
- Information System Operations - Procedures
- Intellectual Property - Academic Policy
- Privacy and Right to Information - Operational Policy
- Privacy Management - Procedures
- Research Data Management - Procedures
- Responsible Research Conduct - Academic Policy
- Right to Information - Procedures
- Risk Management - Governing Policy
- Risk Management - Procedures
- University Audit and Assurance - Governing Policy
- University Policy Documents - Procedures

LINKED DOCUMENTS

- Data Breach - Procedures

- Data Classification - Procedures
- Data Management - Procedures
- Records Management - Procedures

SUPERSEDED DOCUMENTS

- Right to Information - Governing Policy
- Records Management - Governing Policy
- Information Privacy - Governing Policy

RELATED LEGISLATION / STANDARDS

- Right to Information Act 2009 (Qld)
- Public Records Act 2023 (Qld)
- Information Privacy Act 2009 (Qld)