Information Technology Services
29 September 2023

The University of Queensland
Australia
CREATE CHANGE

Information Governance and Management Framework

Metadata for document management

Version	1.2
Approval Authority	USET
Document Custodian	Chief Information Officer
Last Approval Date	25 August 2023
Next Review Date	25 August 2026
Audience / Users	UQ all
Information Security Classification	OFFICIAL-PUBLIC
Notes	

Contents

1. Purpose

UQ's information is a valued asset that underpins effective and efficient operations and plays a growing role in shaping UQ's strategic direction. As our reliance on data and information increases, controlled access to well-understood and high-quality information is critical. To achieve this, clear and effective information governance structures and practices must be implemented.

The Information Governance and Management Framework provides a consistent approach to information governance and management at The University of Queensland (UQ). This document defines our information governance and management roles, authorities, and structures to:

- support UQ's strategic objectives,
- ensure UQ protects and preserves its information in line with UQ's Enterprise Risk Management Framework,
- enable effective, ethical, and secure use of information, and
- meet legislative and administrative obligations.

This framework supports UQ's Information Management Policy.

2. Scope

This framework applies to all UQ data, information and records. Individuals who use, create or access UQ information must comply with this framework. This includes but is not limited to:

- staff
- contractors and consultants
- students and visitors (with regards to UQ information, i.e. not information they generate as part of their studies or attending an event)
- title holders and third parties.

3. Legislative obligations

The University is required to meet legislative obligations that relate to the management of data and information across administration, teaching and learning and research. The following instruments contain provisions relevant to the management of information across its lifecycle and applies to all information held by UQ. Note that certain instruments will apply to different extents, and to different information depending on the context.

See the Compliance legislation register for more information.

3.1 Commonwealth instruments

- Broadcasting Services Act 1992
- Copyright Act 1968
- Cybercrime Act 2001
- Education Services for Overseas Students Act 2000
- Electronic Transactions Act 1999

- Privacy Act 1988
- Spam Act 2003
- Telecommunications (Interception and Access) Act 1979
- Telecommunications Act 1997
- Security of Critical Infrastructure Act 2018
- Data Availability and Transparency Act 2022
- Education Services for Overseas Students Regulations 2001
- Tertiary Education Quality and Standards Agency Act 2011
- National Code of Practice for Providers of Education and Training to Overseas Students 2018
- Higher Education Standards Framework (Threshold Standards) 2021.

3.2 Queensland instruments

- Information Privacy Act 2009
- Public Records Act 2002
- Right to Information Act 2009
- University of Queensland Act 1998
- Information Access and Use Policy (IS33)
- Information Asset Custodianship Policy (IS44)
- Information Governance Policy
- Information Security Policy (IS18:2018)
- Metadata (IS34)
- Records Governance Policy
- Queensland retention and disposal schedules: University Sector Retention and Disposal Schedule (QDAN 601), the General Retention and Disposal Schedule (GRDS), and the General Retention and Disposal Schedule for Digital Source Records.

3.3 Additional obligations

At various times, and with respect to certain information, UQ may also have obligations under international privacy laws (such as the European Union's General Data Protection Law). Accreditations, partnerships, or agreements may also carry additional obligations.

3.4 Supporting documents

The following frameworks, policies and procedures support the application of this framework and compliance with applicable legislative obligations:

- Information Management Policy
- Information Security Classification Procedure
- Data Handling Procedure
- Destruction of Physical Records Procedure

- Access to and Amendment of UQ Documents Procedure
- Keeping Records at UQ Procedure
- Enterprise Data Ethics Framework
- Cyber Security Policy
- Privacy Management Policy
- Cyber Security Incident Management Procedure (*local IT operating procedure)*.

Information domain and information entity-specific policies, procedures or rules may be available depending on the business area. The University will seek to mature this documentation across business areas.

4. Information governance

Information governance defines the roles and responsibilities, decision rights, controls, and processes used to manage information at UQ.

4.1 Information categorisation

Information is grouped into **information domains**. Each domain contains **information entities,** which are groups of information related to that information domain. Each information domain will be assigned to an Information Domain Custodian and Information Leader (who oversees a group of domains based on organisational structures). For more information, view the information entity catalogue.

The following diagram shows how information is categorised at UQ.

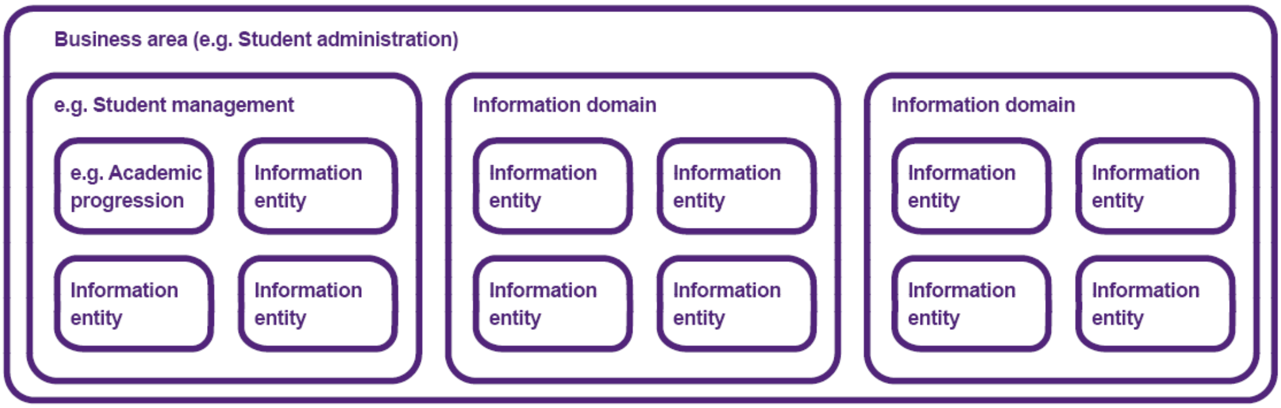
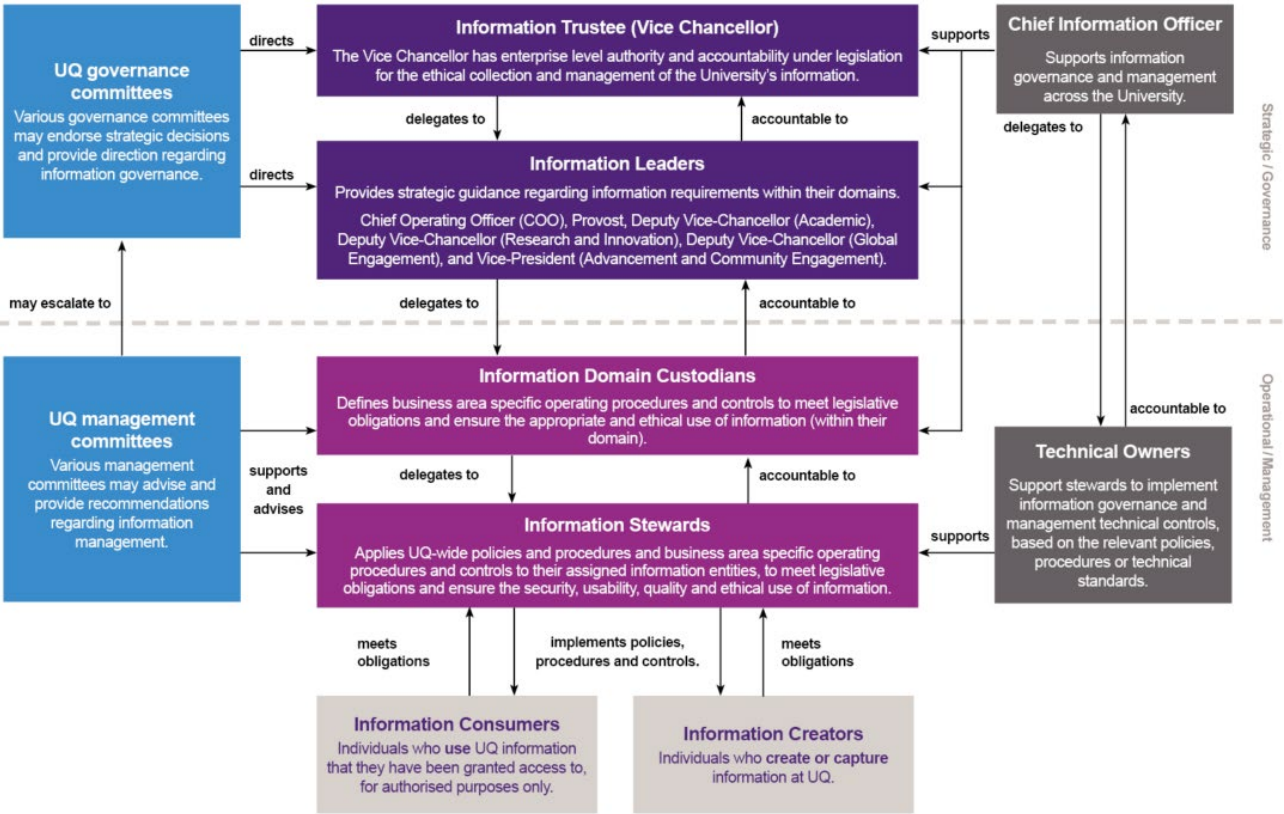


Figure 1 – Diagram illustrating how information is grouped into entities and domains

4.2 Decision rights

Clearly defined decision rights enable efficient decision making regarding the management of data and information through its lifecycle. The decision rights model outlines a hierarchy of relationships, describes levels of accountability and responsibilities, and provides a reference point for information governance decisions. Note that they aren't necessarily reflective of UQ's organisational structure.

Figure 2 - Decision rights model (also known as Information Governance model)



UQ governance committees
Various governance committees may endorse strategic decisions and provide direction regarding information governance.

Information Trustee (Vice Chancellor)
The Vice Chancellor has enterprise level authority and accountability under legislation for the ethical collection and management of the University's information.

Chief Information Officer
Supports information governance and management across the University.

Information Leaders
Provides strategic guidance regarding information requirements within their domains.
Chief Operating Officer (COO), Provost, Deputy Vice-Chancellor (Academic), Deputy Vice-Chancellor (Research and Innovation), Deputy Vice-Chancellor (Global Engagement), and Vice-President (Advancement and Community Engagement).

UQ management committees
Various management committees may advise and provide recommendations regarding information management.

Information Domain Custodians
Defines business area specific operating procedures and controls to meet legislative obligations and ensure the appropriate and ethical use of information (within their domain).

Technical Owners
Support stewards to implement information governance and management technical controls, based on the relevant policies, procedures or technical standards.

Information Stewards
Applies UQ-wide policies and procedures and business area specific operating procedures and controls to their assigned information entities, to meet legislative obligations and ensure the security, usability, quality and ethical use of information.

Information Consumers
Individuals who **use** UQ information that they have been granted access to, for authorised purposes only.

Information Creators
Individuals who **create or capture** information at UQ.

4.3 Roles and responsibilities

The roles and responsibilities relevant to the governance, collection, management, and use of information are listed below.

4.3.1 Information Trustee (Vice-Chancellor)

The Information Trustee at UQ is the Vice-Chancellor.

The Vice-Chancellor has enterprise level authority and accountability under legislation for the collection and management of the University's information.

As Information Trustee the Vice-Chancellor is accountable for ensuring the collection and management of UQ's information and records in accordance with relevant legislative, regulatory and policy obligations.

As Information Trustee the Vice-Chancellor is responsible (but may delegate that responsibility) for:

- ensuring information is managed and governed as a strategic asset across the University,
- approving University-wide policies to ensure the security, confidentiality and privacy of information is protected in accordance with legislation and ethical standards, and
- assigning Information Leaders to the University's information domains.

4.3.2 Information Leader

Information Leaders provide strategic guidance regarding information requirements for information domains within their respective business areas.

At UQ, the Information Leaders are:

- Chief Operating Officer
- Provost
- Deputy Vice-Chancellor (Academic)
- Deputy Vice-Chancellor (Research and Innovation)
- Vice-President (Advancement and Community Engagement).

For each of their assigned information domains, Information Leaders are responsible for:

- Assigning Information Domain Custodians to define key information management decisions and directions (for their domain).
- Providing strategic direction to Information Domain Custodians regarding the quality, security, integrity, accuracy, consistency, privacy, confidentiality and accessibility of, and ethical use of information across its lifecycle.
- Acting as a champion for information governance and information-related initiatives.
- Promoting awareness and understanding of information governance across UQ.
- Endorsing operating procedures and controls associated with managing the University's information specific to their information domains.

4.3.3 Information Domain Custodian

An Information Domain Custodian is assigned to one or more information domains (see the information entity catalogue for more details). For example, the Chief human Resources Officer is the Information Domain Custodian for the Human Resources domain.

For each assigned information domain, the Information Domain Custodian is responsible for:

- Defining business area specific (e.g. Research) operating procedures and controls to ensure legislative and policy obligations are met, and to ensure the confidentiality, integrity, availability and appropriate and ethical use of information.
- Key information management decisions and directions:
  - managing escalated risks related to information in alignment with the Enterprise Risk Management Framework,
  - approving archival requests for high risk, high value, vital and permanent retention records,
  - endorsing disposal requests for records for approval by the Records Governance Manager,
  - assigning Information Stewards to oversee day to day information management,
  - making decisions as required based on escalations from Information Stewards, and
  - approving privacy impact assessments for systems and processes within their information domain.

4.3.4 Information Steward

An Information Steward is assigned to one or more information entities. For example, the Director, People Services in the Information Steward for the Staff, Worker, Leave and Timesheet information entities (within the Human Resources domain).

For each assigned entity, the Information Steward is responsible for:

- Providing advice and making decisions regarding day-to-day management of information.
- Implementing UQ-wide and business area specific decisions, policies, procedures, and standards, to ensure legislative and policy obligations are met. This includes (but is not limited to):
  - reviewing and approving data access requests (e.g. data sharing agreements),
  - ensuring controls are applied to protect the confidentiality, integrity and availability of information,
  - setting and/or endorsing an overall information security classification for each information entity,
  - applying UQ-wide policies and procedures and business area specific (e.g. Research) operating procedures and controls to ensure legislative and policy obligations are met,
  - monitoring and continuously improving the quality of information in line with the University's data quality expectations,
  - ensuring information is consistently and accurately captured and classified in the approved information system,
  - providing advice on the appropriate and ethical use and interpretation of information,
  - reviewing and recommending decisions for archiving high risk, high value, vital and permanent retention records, for approval by the Information Domain Custodian, and

- reviewing and recommending decisions for disposal requests of records for endorsement by the Information Domain Custodian, prior to final approval by the Records Governance Manager.

4.3.5 Information Creators

Information Creators create or capture information at UQ. An Information Creator is responsible for:

- accurately and ethically creating and capturing information and data,
- ensuring the appropriate information security classification is assigned (in accordance with direction from Information Stewards) when information is created or captured,
- complying with relevant legislation as well as UQ-wide and business area specific policies, procedures, and controls, and
- seeking advice on information requirements from the relevant Information Steward.

4.3.6 Information Consumers

Information Consumers use UQ information that they have been granted access to, for authorised purposes only. Information Consumers are responsible for:

- using the University's information in compliance with all relevant legislation as well as UQ-wide and business area specific policies, procedures and controls,
- using the University's information ethically and securely while respecting confidentiality and privacy,
- ensuring the information they consume is fit for its specific purpose/s, and
- providing feedback about the quality of information to relevant Information Stewards.

4.3.7 Chief Information Officer

The Chief Information Officer (CIO) is accountable for:

- establishing and implementing information governance structures,
- developing and maintaining information management capabilities,
- compliance with legislative instruments as defined in the Compliance legislation register, and
- developing and implementing UQ-wide information management policies, procedures and technical standards to protect UQ's information.

The CIO is responsible for:

- developing IT strategies and roadmaps, and the approval of IT initiatives that continuously improve information governance and management,
- ensuring that Technical Owners are adequately resourced to fulfil their responsibilities, and
- ensuring that information roles (i.e. Information Leaders, Information Domain Custodians and Information Stewards) are assigned across UQ.

4.3.8 Technical Owner

A Technical Owner is the staff member responsible for the ongoing management of a service or asset from a technical perspective (including in relation to managing third party-provided services).

Technical Owners are responsible for:

- Supporting Information Stewards to implement information governance and management technical controls, based on the relevant policies, procedures or technical standards. This may include updates, patches, technical changes and maintaining any security controls.
- Conducting privacy impact assessments for the implementation of new systems or processes (or changes to existing systems or processes) as and when required, and with the assistance of Information Stewards and the Right to Information and Privacy Manager.

4.3.9 Records Governance Team

The Records Governance Team is responsible for:

- advising on and auditing compliance with record keeping obligations,
- recording the existence of vital, high-risk, high-value records (including records that need to be retained permanently),
- maintaining a register of UQ systems approved to retain records,
- advising on the management, treatment, and preservation of vital, high-risk, high-value and permanent retention records,
- developing strategies for records capture, maintenance, lifecycle and archive management, and
- maintaining and implementing record keeping and destruction procedures.

4.3.10 Right to Information and Privacy (RTIP) Office

The RTIP Office is responsible for:

- managing UQ's administrative access schemes and its obligations under the *Right to Information Act 2009* and *Information Privacy Act 2009*, and
- providing advice and leadership in relation to privacy compliance across UQ.

4.3.11 Senior Manager, Data and Identity Services

The Senior Manager, Data and Identity Services is responsible for

- maintaining and implementing this framework, and
- escalating high-rated risks to UQ committees requiring resolution as required.

4.3.12 Data Strategy and Governance Team

The Data Strategy and Governance Team supports the CIO and the Senior Manager, Data and Identity Services to implement and maintain this framework. The team is responsible for:

- Responding to information governance and management legislative and regulatory requirements (under the remit of the CIO, as defined in the Compliance legislation register).
- Reporting to UQ committees on information management compliance as required.
- Providing services to enhance information management and improve information security at UQ. This includes but is not limited to:
    - developing and maintaining UQ's information entity catalogue and supporting data models,
    - facilitating data governance processes (e.g. data sharing agreements and data scoping),
    - ensuring the continuous improvement of information governance and management,

  - developing and delivering data governance training, literacy, and other awareness activities, and
  - maintaining a data governance risk register.

4.3.13 Governance and management committees

UQ has committees in place to provide oversight of information governance at UQ. Please see links below to UQ committees.

- Committees at UQ
- IT Governance and management committees.

Key responsibilities include:

- providing governance oversight of information management,
- ensuring that information management investment is aligned with strategic goals of UQ,
- ensuring UQ protects and preserves its information in line with UQ's Enterprise Risk Management Framework,
- monitoring assurance and compliance across UQ, and
- ensuring adequate information capabilities are in place to support the access and use of UQ information services.

See the Appendix for more information on UQ and IT committees.

5. Information management

Information management is a collection of capabilities delivered through people, processes and technology to support information governance and ensure the confidentiality, integrity, availability, quality and security of our information and data throughout their lifecycle.

5.1 Information lifecycle

Information should be managed consistently from creation to final disposal. The lifecycle involves people, processes and technology and drives improved control over information as it moves through the various lifecycle stages described below.

The information lifecycle at UQ includes the following stages:

- **Plan and design:** information management should be carefully planned, with activities designed to meet University needs and compliance requirements throughout the lifecycle.
- **Create, capture and classify:** Information may be obtained through several means including manual data entry and automatic capture via devices or systems. At the time information is acquired, key metadata should be recorded, including the information security classification.
- **Store and secure**: Information must be stored appropriately, with consideration given to security and access management.
- **Manage and maintain:** Information management is an active process. Information should be managed to maintain its integrity, quality and usability.
- **Share and (re)use**: Sharing and re-use of information requires oversight to ensure it is ethical and compliant with UQ policies and legislative requirements. Information should be discoverable to streamline sharing and re-use for appropriate activities.

- **Retain and archive:** Information should be retained while required and archived in line with any relevant record retention periods.
- **Dispose or destroy**: Information should be destroyed in an appropriate manner at the end of its useful life, ensuring that records are destroyed (or transferred to the appropriate owner) in line with UQ's Keeping Records at UQ Procedure and Destruction of Records Procedure.

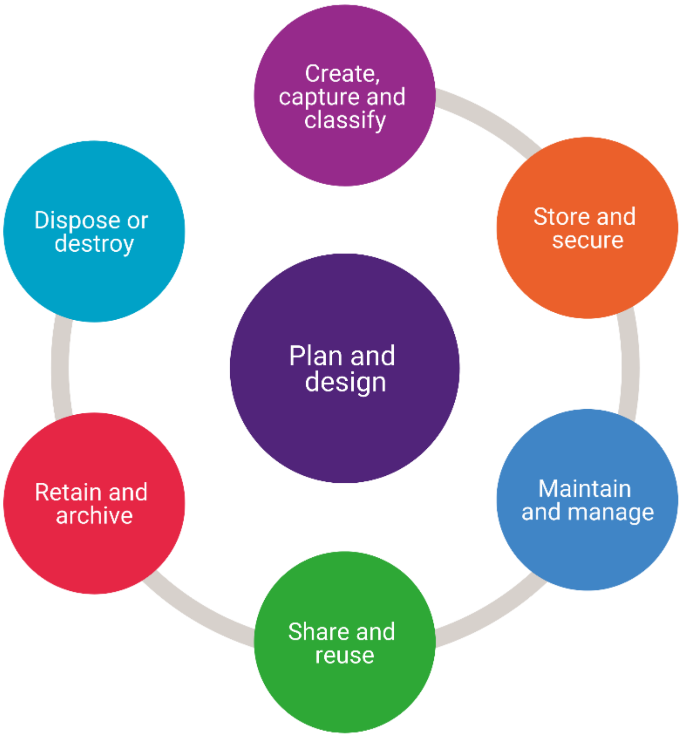


Figure 2 - Information lifecycle diagram

5.2 Information management capabilities

Capability	Description	Supporting documents
Information management planning and design	Information management should be carefully planned, with activities designed to meet University needs and compliance requirements throughout its lifecycle.	• training and resources • data and information knowledge articles • Information Security Classification Procedure • information security classification guidance.
Data management	Appropriate data management controls, protects, delivers and enhances the value of UQ's data.	• file storage guidance • Data Handling Procedure.
Data sharing	Data should be available to the community and accessible within our systems in a controlled, coordinated way.	• file storage guidance • explore and access the data hub • learn more about UQ's central integration platform

		• request access to data (data sharing agreements) • personal information register • UQ publication scheme • disclosure log • Access to and Amendment of UQ documents.
Insights management	Operational and strategic decision-making should be supported by insights derived from an UQ's data.	• UQ Reportal • analytics data services.
Information protection	Information protection should be embedded in University activities and business processes.	• Information Security Classification Procedure • information security classification guidance • learn about data privacy and your responsibilities • guide to personally identifiable information (PII) and confidential information • Application Security Standard • Access and Privileges Management Framework.
Records management	Records must be managed throughout their lifecycle, in compliance with the *Public Records Act 2002* and UQ's records management requirements.	• records governance information • Keeping Records at UQ Procedure • Destruction of Records Procedure.

Appendix A

1. Information on UQ and IT committees

- **University Senior Executive Team (USET):** the USET approves information management frameworks and policies.
- **Senate Risk and Audit committee:** The Senate Risk committee defines UQ's risk appetite statement (RAS), which impacts information risk management approaches. This committee also receives reports relating to IT risks, including cyber security and information management.
- **Vice-Chancellor's Risk and Compliance Committee (VCRCC):** the VCRCC receives reports relating to IT risks, including cyber security and information management.
- **IT Policy, Risk and Assurance Committee (IT PRAC):** the IT PRAC has oversight of IT risk management, policy review and endorsement, and compliance monitoring. The committee also endorses the annual IT top 10 risks, reports these risks up to the VCRCC, and monitors progress of risk treatment actions. For more information, refer to the IT Governance and Management Framework.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Contact details

Data Strategy and Governance
E datagovernance@uq.edu.au
W data.uq.edu.au

CRICOS Provider Number 00025B