Office of the Chief Information Officer
9 February 2022

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Information Governance and Management Framework

Metadata for document management

Version	1.1
Approval Authority	Chief Information Officer
Document Custodian	Chief Information Officer
Last Approval Date	09 February 2022
Next Review Date	05 August 2024
Audience / Users	UQ all
Information Security Classification	OFFICIAL-PUBLIC
Author	Mr. Sasenka Abeysooriya
Notes	

Contents

1. Document structure 5
1.1 Information Governance 5
1.2 Information Management 5
2. Purpose and context 6
2.1 Scope 6
3. Information Governance and Management Framework 6
3.1 Vision for information 6
3.2 Principles 6
3.3 Obligations 7
3.3.1 Federal Acts 7
3.3.2 Queensland Acts 7
3.3.3 Federal Policies 7
3.3.4 Queensland Policies 7
3.3.5 UQ Policies and Procedures 7
4. Information Governance 9
4.1 Governance context 9
4.2 Decision rights 9
4.3 Roles and responsibilities 12
4.3.1 Information Trustee 12
4.3.2 Information Leader 12
4.3.3 Information Domain Custodian 12
4.3.4 Information Stewards 13
4.3.5 Information Creators 13
4.3.6 Information Consumer 14
4.3.7 Chief Information Officer 14
4.3.8 Information Service Providers 14
4.3.9 Governance Bodies 15
4.4 Governance controls 15
5. Information Management 18
5.1 Information Lifecycle Management 18
5.2 Information Management Capabilities 19
5.2.1 Information planning and design 20
5.2.2 Data management 20
5.2.3 Data sharing 21
5.2.4 Information protection 21
5.2.5 Enterprise content management 21
5.2.6 Records management 22
5.2.7 Insights management 22

Tables

Table 1 - RACI definitions 10
Table 2 - RACI chart for high-level information governance and management activities 11
Table 3 - Information planning and design capabilities 20
Table 4 - Data management capabilities 21

Table 5 - Data sharing capabilities 21
Table 6 - Information protection capabilities 21
Table 7 - Enterprise content management capabilities 22
Table 8 - Records management capabilities 22
Table 9 - Insights management capabilities 22
Table 10 - Governance controls 32

Figures

Figure 1 - Information Governance and Management Framework document structure 5
Figure 2 - Decision rights model (also known as Information Governance model) 9
Figure 3 - Information Lifecycle Management diagram 18

Appendices

Appendix A Decision rights example
Appendix B Governance controls
Appendix C Information Lifecycle Management examples

1. Document structure

The Information Governance and Management Framework (the Framework) provides a consistent enterprise approach to information governance and information management across The University of Queensland (UQ). The document describes our obligations throughout the information lifecycle (as described in section 5.1) and describes the governance and management structures and decision rights.

The framework supports UQ's Information Management Policy.

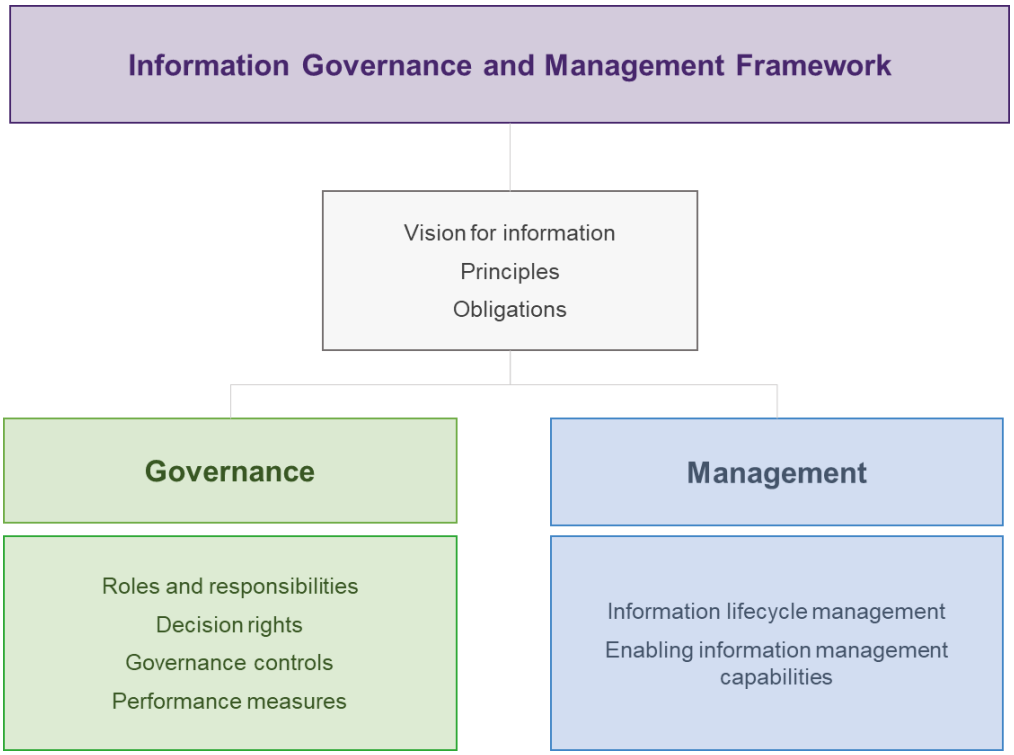


Figure 1 - Information Governance and Management Framework document structure

1.1 Information Governance

Information governance is a collection of policies, practices and processes that provides a formal framework to establish decision rights and apply control through defined roles and responsibilities for the management of information and data assets [1]throughout their lifecycle.

1.2 Information Management

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

[1] An Information or Data Asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.
*Note: and Information or Data Asset can be in the form of an information sub-domain, collection of datasets, data elements, and so on.

2. Purpose and context

The University of Queensland (UQ) is committed to appropriately managing all forms of information that it creates and holds. Effective information management ensures that the right information is available to the right person, in the right format, at the right time. To achieve this, necessary controls must be asserted over our information assets with the support of clear and effective information governance practices.

The Information Governance and Management Framework (the Framework) outlines a shared overarching approach to information governance and management at UQ.

2.1 Scope

This Framework applies to all University staff, students and users of the University's information resources including contractors, third-party agents of the University and any other University affiliate who is authorised to access institutional data or information. It covers information resources hosted on-campus or externally.

The framework may be used to benchmark current information management practices and to identify aspects of information management and governance that require capability improvement.

3. Information Governance and Management Framework

3.1 Vision for information

The University of Queensland operates effectively and efficiently when members of the University community have access to the correct information at the time that they need it. Information management and governance is about maturing practices and creating a culture that ensures appropriate oversight is in place to properly manage and maintain our information assets.

Our vision for information management and governance is that:

- information is managed in line with statutory and administrative obligations
- information management supports and aligns with organisational drivers, University needs and strategic objectives
- custodianship and stewardship of information is improved
- the ability for information to be used and valued as an operational and strategic asset is increased
- information is managed in a way that enables it to be used effectively, ethically and securely
- information is managed according to its purpose and associated risk profile
- appropriate controls are in place to secure our information.

3.2 Principles

- Information is treated as an asset.
- Information can be found and accessed.
- Information is suitable for all of its uses.
- Information remains compliant.
- Information privacy, confidentiality and security is assured.

Refer to the UQ Information Management Policy for a detailed description of the principles.

3.3 Obligations

The University is required to meet legislative and regulatory requirements that relate to the management of data and information across all of the high-level domains of administration, teaching and learning and research. The following legislation and policies contain provisions relevant to the management of information across its lifecycle and applies to all information held by the organisation.

3.3.1 Federal Acts

- Broadcasting Services Act 1992
- Copyright Act 1968
- Cybercrime Act 2001
- Education Services for Overseas Students Act 2000
- Electronic Transactions Act 1999
- Evidence Act 1995
- Privacy Act 1988
- Public Interest Disclosure Act 2013
- Spam Act 2003
- Telecommunications (Interception and Access) Act 1979
- Telecommunications Act 1997

3.3.2 Queensland Acts

- Information Privacy Act 2009
- Public Records Act 2002
- Right to Information Act 2009
- University of Queensland Act 1998

3.3.3 Federal Policies

- Education Services for Overseas Students Regulations 2001
- National Code of Practice for Providers of Education and Training to Overseas Students 2018

3.3.4 Queensland Policies

- 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 State Archives authorised disposal schedules: University Sector Retention and Disposal Schedule (QDAN 601)
    - General Retention and Disposal Schedule (GRDS)

3.3.5 UQ Policies and Procedures

- Information Management Policy
- Information Governance and Management Framework (this document)
- Information Security Classification Procedure
- Data Handling Procedure
- Enterprise Data Ethics Framework
- Cyber Security Incident Management Procedure
- Cyber Security Policy
- Privacy Policy
- Destruction of Physical Records Procedure

Some aspects of international legislations such as the General Data Protection Regulation (GDPR) may apply to UQ. The GDPR and the Australian Privacy Act 1988 share many common requirements.

Information Governance

4. Information Governance

Information governance defines the roles and responsibilities, decision rights and the controls and processes required to effectively manage information collected and/or held by the University.

4.1 Governance context

UQ's institutional data and information are a valued asset that underpins effective and efficient operations. Insights from data play a growing role in shaping the strategic direction of our University. As our reliance on data and information increases, controlled access to well-understood and high-quality data and information is critical. A successful future for UQ relies on the ability to grow capabilities to leverage data and information while ensuring that the University is able to assert necessary controls over it, with the support of clear and effective information governance practices.

4.2 Decision rights

Clearly defined decision rights[2] across the University is a key enabler of good information governance to support efficient decision making regarding the management of data and information through its lifecycle. The decision rights model outlines a hierarchy of relationships describing levels of accountability and responsibilities, and provides a reference point for information governance decisions. An example of how this works in practice is given in Appendix A.

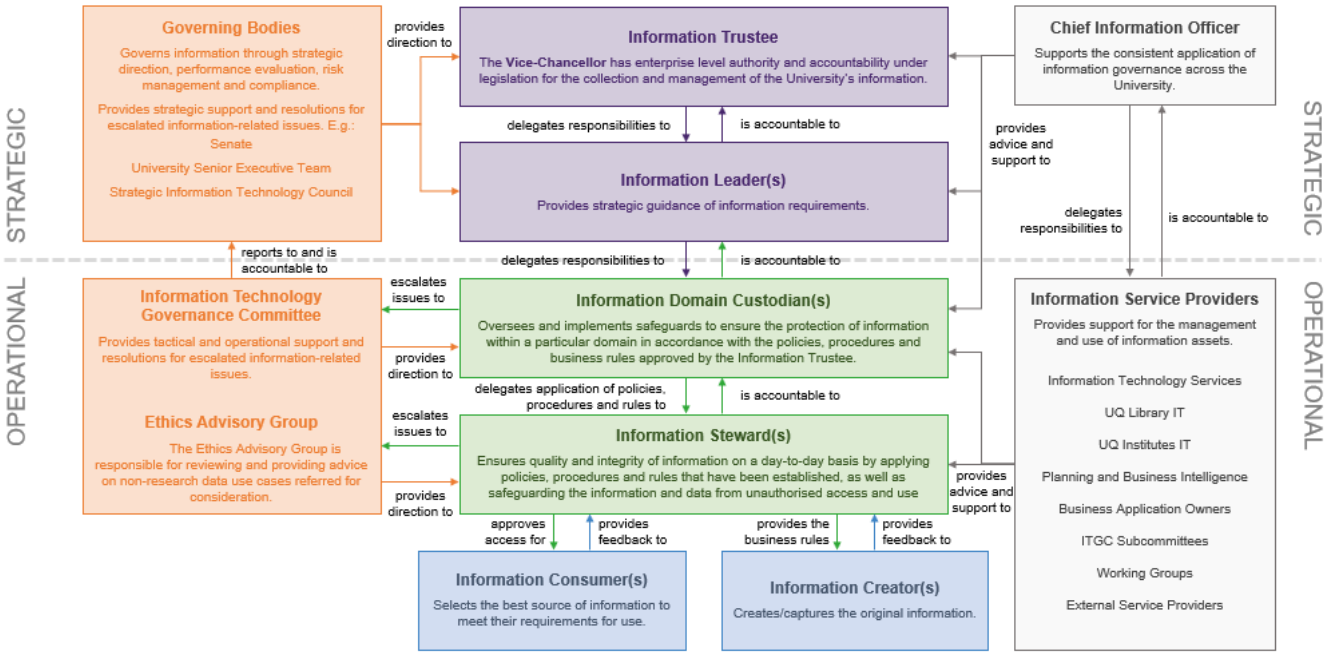


Figure 2 - Decision rights model (also known as Information Governance model)

The following table (table 1), describes the types of involvement necessary to inform the RACI table (Responsible, Accountable, Consulted and Informed) (table 2) which includes the high-level activities required to manage our enterprise data governance landscape.

[2] 'Decision rights' are decision making structures that aren't necessarily reflective of UQ's organisational structure.

RACI	Description
RACI - Accountable	The one ultimately answerable for the correct and thorough completion of the activity or task, and the one who delegates the work to those responsible. An accountable person must sign off (approve) work that a responsible person completes. There must be only one accountable person specified for each task or deliverable.
RACI - Responsible	Those who do the work to achieve the activity or task. There is at least one role with a participation type of responsible person(s), although others can be delegated to assist in the work required.
RACI – Consulted	Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication.
RACI – Informed	Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

Table 1 - RACI definitions

The following table defines the high-level activities required to manage our enterprise data governance landscape. It outlines who is accountable, responsible, contributing and informed and how often the activities should be reviewed.

Each activity is either a Planning activity (P) or a Control activity (C).

Activities	Information Trustee	Information Leader	Information Domain Custodian	Information Steward	Information Consumer	Information Creator	Chief Information Officer	Information Service Provider	Senate	UQ Senior Executive Team	UQ Senior Leaders Group	Strategic Information Technology Council	Information Technology Governance Committee	Ethics Advisory Group
Compliance with all legal, regulatory, and policy requirements (including University, state and federal) (P)	A	R	R	R	R	R	R	R	R	R	R	R	R	C
Strategic direction, policies and standards relating to the management of information (P)	A	R	C	C	I	I	R	C	R	R	C	C	C	I

Activities	Information Trustee	Information Leader	Information Domain Custodian	Information Steward	Information Consumer	Information Creator	Chief Information Officer	Information Service Provider	Senate	UQ Senior Executive Team	UQ Senior Leaders Group	Strategic Information Technology Council	Information Technology Governance Committee	Ethics Advisory Group
Identify and assign information and data governance custodian and stewardship roles (P)	R	R	C	C	I	I	A	C	I	I	I	I	I	I
Policies, procedures and rules to manage information and data across the lifecycle (P)	A	R	R	C	I	I	R	C	I	I	I	I	I	I
Collection, management, use and disposal of University's information and data (C)	A	R	R	R	R	R	R	R	I	I	I	I	I	I
Manage and resolve data related conflicts, risks and issues (C)	A	R	R	R	C	C	R	R	I	R	R	R	R	I
Communicate and monitor compliance with policies, procedures and rules (C)	R	R	R	R	R	R	A	R	I	R	R	R	R	I
Approve the release of information and data external to the University (C)	A	C	R	C	C	C	R	C	I	I	I	I	I	I
Assess, measure, improve and/or remediate data performance and quality (C)	R	R	R	R	R	R	A	R	I	R	R	R	R	I
Approve the retention and destruction of University records (C)	A	I	R	I	I	I	C	C	I	I	I	I	I	I

Table 2 - RACI chart for high-level information governance and management activities

4.3 Roles and responsibilities

Information governance roles and responsibilities exist to champion the vision for information management, build an information aware culture and ensure fit for purpose information is maximised to achieve value across the University. The recommended governance roles and responsibilities crucial to the overall collection, management and use of information are listed below.

4.3.1 Information Trustee

The Information Trustee (also referred to as the Information Owner) at UQ is the Vice-Chancellor.

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

The Information Trustee may delegate responsibilities to the Information Leaders or other parties.

The Information Trustee is accountable for:

- the collection and management of the University's information in accordance with relevant legislative, regulatory and policy obligations.

The Information Trustee is responsible (but may delegate that responsibility) for:

- approving the release of the University's information external to the University (e.g. government reporting, media or the public)
- ensuring information is managed and governed as a strategic asset across the University
- ensuring the security, confidentiality and privacy of information is protected in accordance with legislation and ethical standards
- ensuring that information and records retention and destruction obligations and authorisations have been delegated to Information Custodians
- approving University-wide policies, procedures and rules associated with governing and managing information (within the delegation of the Vice Chancellor, noting that some policies are reserved for Senate approval)
- approving and supporting business cases relating to information management investments
- assigning Information Leaders to the University's high-level information domains.

4.3.2 Information Leader

Information Leaders provide strategic guidance regarding information requirements within one or more information domains.
.

An Information Leader is responsible for:

- providing direction 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 the University
- approving the policies, procedures and rules associated with managing the University's information specific to a functional area.

4.3.3 Information Domain Custodian

Information Domain Custodians (Information Custodian) define and implement safeguards to ensure the protection and ethical compliance of information within their domain. This must be done in accordance with the policies, procedures and rules approved by the Information Trustee or Information Leader.

An Information Domain Custodian is responsible for:

- defining the information domain[3] specific procedures and rules to ensure proper quality, security, integrity, consistency, privacy, confidentiality and accessibility of information throughout its lifecycle
- ensuring information is managed in compliance with relevant legislation, policy and standards
- ensuring good records management practices are followed throughout the information lifecycle
- managing and maintaining information within their domain, including metadata, to ensure that discovery mechanisms function
- managing escalated risks related to domain-specific information through the University's risk management processes
- assuring the quality and integrity of information in their domain in line with relevant quality standards
- monitoring and responding to performance measures for their information domains
- approving the release of information, based on criteria approved by the Information Trustee, to external parties
- ensuring that requests for archiving and disposal of information/records are approved/denied in accordance with University policies and procedures
- assigning Information Stewards to oversee day to day information management.

4.3.4 Information Stewards

Information Stewards are responsible for the quality, integrity and ethical use of information within an information sub-domain[4] on a day-to-day basis. An Information Steward may manage information within multiple information sub-domains.

The stewards apply relevant policies, procedures and rules, including safeguarding the information from unauthorised access and abuse.

An Information Steward is responsible for:

- the application of relevant legal, policy and standards requirements
- the application of security, confidentiality and privacy requirements
- the implementation of strategies for quality improvement and resolving quality issues
- monitoring and continuously improving the quality of information in line with the University's data quality expectations
- ensuring information is consistently and accurately captured in the approved information system
- providing advice on the proper use and interpretation of information
- reviewing and approving (or rejecting) requests for access to data and information
- reviewing and recommending decision for archiving and disposal requests of information and records
- assuring that information complies with all legal, regulatory and policy requirements.

4.3.5 Information Creators

Information Creators capture or create the information as defined by the Information Domain Custodian.

An Information Creator is responsible for:

- accurately capturing information and data in line with legislation, policy and standards
- complying with all information governance policies, procedures, processes and rules
- seeking advice on information requirements and providing feedback to the appropriate Information Steward.

[3] An Information Domain is a broad category or theme under which UQ information can be identified and managed.
[4] An Information Sub-Domain is a specific group of information that is related to an Information Domain.

4.3.6 Information Consumer

Information Consumers select the best source of information to meet their requirements for use.

Information Consumers are responsible for:

- using the University's information and data assets to which they have been granted access, and only for the purposes approved, in line with all relevant information-related legislation, policies, procedures and processes
- using the University's information and data assets ethically and securely while respecting confidentiality and privacy of the assets
- defining what makes the information fit for purpose as it is important the information meets requirements
- providing feedback about the information to relevant Information Stewards.

4.3.7 Chief Information Officer

The Chief Information Officer (CIO) is accountable for:

- developing and maintaining the information management priorities
- understanding the data security needs and implementing appropriate controls
- developing information policies, standards and procedures.

The CIO is responsible for:

- interpreting the business and information needs, and strategic goals of UQ and translating them into ICT initiatives that deliver valued information assets to UQ
- supporting the Information Trustee and Information Leaders in setting the strategic direction for UQ's ICT and information management
- ensuring that Information Service Providers are adequately resourced to support the Information Stewards and Custodians to fulfil their responsibilities
- ensuring that appropriate mitigation, reparation and punitive measures are taken following investigations of misuse (e.g. the suspension of user accounts)
- ensuring that the Information Management Policy and supporting frameworks and procedures are enforced, maintained and alleged breaches are investigated
- ensuring that an Information Domain Custodian is assigned to each information domain.

4.3.8 Information Service Providers

Information Service Providers (ISP) provide support to embed and implement governance controls and processes. This group includes the technical teams that provide system support and manage access to information including our information systems[5].

The ISPs at UQ include (but are not limited to):

- Information Technology Services
- UQ Library IT
- UQ Schools/Institutes IT
- Planning and Business Intelligence
- Business Application Administrators
- ITGC subcommittees
- working groups

[5] An information system is a place where a collection of data is stored and used for University business functions. An information system is often also a system of record and should therefore fulfil all information lifecycle management requirements from collection all through to disposal. Refer to section 5.1.

- external service providers
  (with all external service providers, an internal UQ service provider must take full responsibility to ensure the external provider fulfils all requirements as required by an ISP).

4.3.9 Governance Bodies

Although the following University boards and committees may not have direct responsibility for information governance, it is essential that they are informed of information governance initiatives which impact their individual charters.

4.3.9.1 Information Technology Governance Committee

The Information Technology Governance Committee (ITGC) governs information through strategic direction, performance evaluation, risk management and compliance. The ITGC provides tactical and operational support and resolution of escalated information governance issues.
Terms of Reference

4.3.9.2 Ethics Advisory Group

The Ethics Advisory Group is responsible for reviewing and providing advice on non-research data use cases referred for consideration. More information about the Ethics Advisory Group is available by contacting the Data Strategy and Governance team via email on datagovernance@uq.edu.au.

4.3.9.3 Strategic Information Technology Council

The Strategic Information Technology Council (SITC) governs information through strategic direction, performance evaluation, risk management and compliance. The SITC provides strategic support and resolution of escalated information-related issues.
Terms of Reference

4.3.9.4 University Senior Executive Team

The University Senior Executive Team (USET) is the senior management forum of the University. The USET provides guidance and oversight of matters that support the strategic priorities of the University, including: key operational matters, the performance of the University against key performance indicators and the governance of the University. The USET also provides advice with respect to decisions made under the exercise of the Vice-Chancellor's delegation.

Issues and/or decision that could not be resolved by the SITC, may be escalated to the USET.
Terms of Reference

4.3.9.5 Senate

Senate is the peak governing body of the University as constituted by the University of Queensland Act 1998.

The primary role of Senate is to exercise oversight of the University and its affairs. In particular, Senate ensures that the appropriate structures, policies, processes and planning are in place for UQ to effectively manage its activities and achieve its goals.
Terms of Reference

4.4 Governance controls

Information governance controls or business rules are the measures implemented by Information Custodians and Stewards to ensure that information is managed appropriately within the University's regulatory environment.

The level of control applied to the information will be commensurate with the value of the information to the University and the risks associated with collection, use and exposure of the information. Enterprise level

controls are applicable to all University information (e.g. except for exempted data sets for regulatory reporting requirements, data should be de-identification of personal information prior to external sharing), and business level controls applicable to information domains (e.g. HR, Finance or Local Laws).

Processes to enforce the controls can be automated, manual, or technology-enabled manual processes. Processes are the methods used to apply governance controls and manage the information.

See Appendix B for a complete list of governance controls mapped to UQ's information lifecycle.

Information Management

5. Information Management

Information management at UQ is enabled through a range of capabilities that are applied throughout the information lifecycle. UQ's information management capabilities are in line with the industry standard 'Business Reference Model' (Capability Model) developed by the Council of Australasian University Directors of Information Technology (CAUDIT).

5.1 Information Lifecycle Management

Information lifecycle management is the consistent management of information from creation to final disposition. It is enabled through people, process 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 steps:

- **plan and design information appropriately;**

- **Create, capture and classify** information adequately
- **store and classify and secure** information appropriately
- **manage and maintain** information in line with external and internal policies and expectations
- **share and (re)use** information where appropriate
- **retain and archive** information for a minimum period
- **dispose of and destroy** information correctly.

Figure 3 - Information Lifecycle Management diagram

Information lifecycle management at UQ is coordinated across the University by the Information Technology Services (ITS) Division.

5.2 Information Management Capabilities

Information management capabilities are delivered through people, processes and technology. Information becomes a discoverable, available, trusted, protected, useful and managed asset of suitable quality through the below capabilities:

- information planning and design
- data management
- data sharing
- information protection
- enterprise content management
- records management
- insights management.

These capabilities and what they entail are further outlined below.

5.2.1 Information planning and design

Information should be consciously planned and designed to meet internal business and governance requirements. To achieve this, information planning and design should encompass the following:

Information needs assessment	• Assessment of the information that the organisation needs to design, make and keep. • Identification of where information requirements need to be built into process, system, service or contract design.
Information risk assessment	• Identification of where risks to information exist in corporate environments, processes, capabilities or services. • Identification of policy and compliance risks. • Implementation of plans to mitigate these risks.
Information architecture	• Assessment of the architecture needed to support information creation, use, governance and management. • Alignment of information management needs to enterprise architecture and future conceptual architecture planning.
Data modelling and design	• Assessment, design and development of the data required to support current and future business needs.
Information lifecycle planning	• Identification of the requirement and processes needed to support digital continuity of information/records, to give assurance of their ongoing authenticity, accessibility and readability over the period they are required to be legally kept. • Alignment of systems, services, processes, capabilities and requirements to support information creation, management, use and disposal.
Information asset registration	• Identification and documentation of core information assets and systems.

Table 3 - Information planning and design capabilities

5.2.2 Data management

Data should be managed with the assistance of plans, programs and practices that control, protect, deliver and enhance the value and management of data assets. To achieve this, data management should encompass the following:

Reference and master data management	• Identification and management of the core data entities (e.g. student, course, research project) and reference data sets (e.g. country codes, field of research codes, classification codes) used across an organisation. • Matching and resolution of data entities captured in multiple sources (this also supports some aspects of identity management).
Metadata management	• Establishment of policies, rules and practices to ensure metadata definition, capture, access, integration, linking, sharing, maintenance and analysis.
Data quality management	• Processes and technologies to assess and improve the quality of organisational data.
Data storage	• Planning, management and coordination of data storage environments.
Information classification	• Identification, organisation and classification of information and information systems to enable their appropriate use and protection. • Note: this capability/aspect is supported by metadata management.

Table 4 - Data management capabilities

5.2.3 Data sharing

Data should be available to the community and within our systems in a controlled, coordinated way. To achieve this, data sharing should encompass the following:

Data Integration and Interoperability	• Processes and technology for managing the controlled sharing of data between applications. This includes the acquisition, extraction, transformation, movement, delivery, replication, federation, virtualisation and operational support for data movement. • Governance and monitoring of data sharing arrangements.
Information search and discovery	• Making data and information from multiple environments available for coordinated searching and controlled access.
Data opening and public release	• Processes to ensure data is made available for public use and reuse. • Development of governance and control processes to ensure personal and sensitive information is protected in open data arrangements. • Community and business liaison to ensure information is released that meets current and future community needs and expectations.

Table 5 - Data sharing capabilities

5.2.4 Information protection

Information protection should be embedded in University activities and business processes. To achieve this, information protection should encompass the following:

Information access management	• Arrangements to ensure access to information is controlled, monitored and appropriate to risk and business requirements. • Application of processes to maintain currency and appropriateness of access and restriction arrangements, including during staff on boarding, off boarding or movement within the organisation. • Development of monitoring processes for information access arrangements.
Privacy management	• Development and implementation of privacy by design approaches to support compliant and effective information design, use and management. • Adoption of processes and practices to support the protection, control and management of personal information.
Cyber security controls	• Identification, risk assessment and management of high value information systems and assets. • Development of governance frameworks to support cyber security for information assets. • Definition of the controls needed to protect high value information assets. • Development and implementation of relevant security by design approaches.

Table 6 - Information protection capabilities

5.2.5 Enterprise content management

Activities and processes should be managed in a way that allows content to be leveraged to enhance innovation. To achieve this, enterprise content management should encompass the following:

Content management	• Tracking and management of information content to enable its appropriate definition, searchability, use and reuse (e.g. websites, knowledgebase, documents).
Digital asset management	• The organisation and management of digital assets to enable their controlled and managed reuse (e.g. digital images used on websites).
University collaboration	• Processes for building and sourcing knowledge from within the University and other national and international universities.
Community collaboration	• Mechanisms for building and sourcing knowledge through collaboration with the community, industry and research sectors.

Table 7 - Enterprise content management capabilities

5.2.6 Records management

Records should be managed throughout the information lifecycle, with processes in place for capturing and maintaining the evidence of, and information about, business activities and transactions in the form of records. To achieve this, records management should encompass the following:

Record creation	• Processes for ensuring appropriate records, and associated metadata, are collected, stored and protected as required to support regulatory, operational, strategic or analytic requirements needs.
Retention and disposal	• Processes to ensure records are kept or disposed of in accordance with legal needs and business requirements (including digital preservation/continuity of accessibility).

Table 8 - Records management capabilities

5.2.7 Insights management

Operational and strategic decision making should be supported by insights derived from an organisation's information and data assets. To achieve this, insights management should encompass the following:

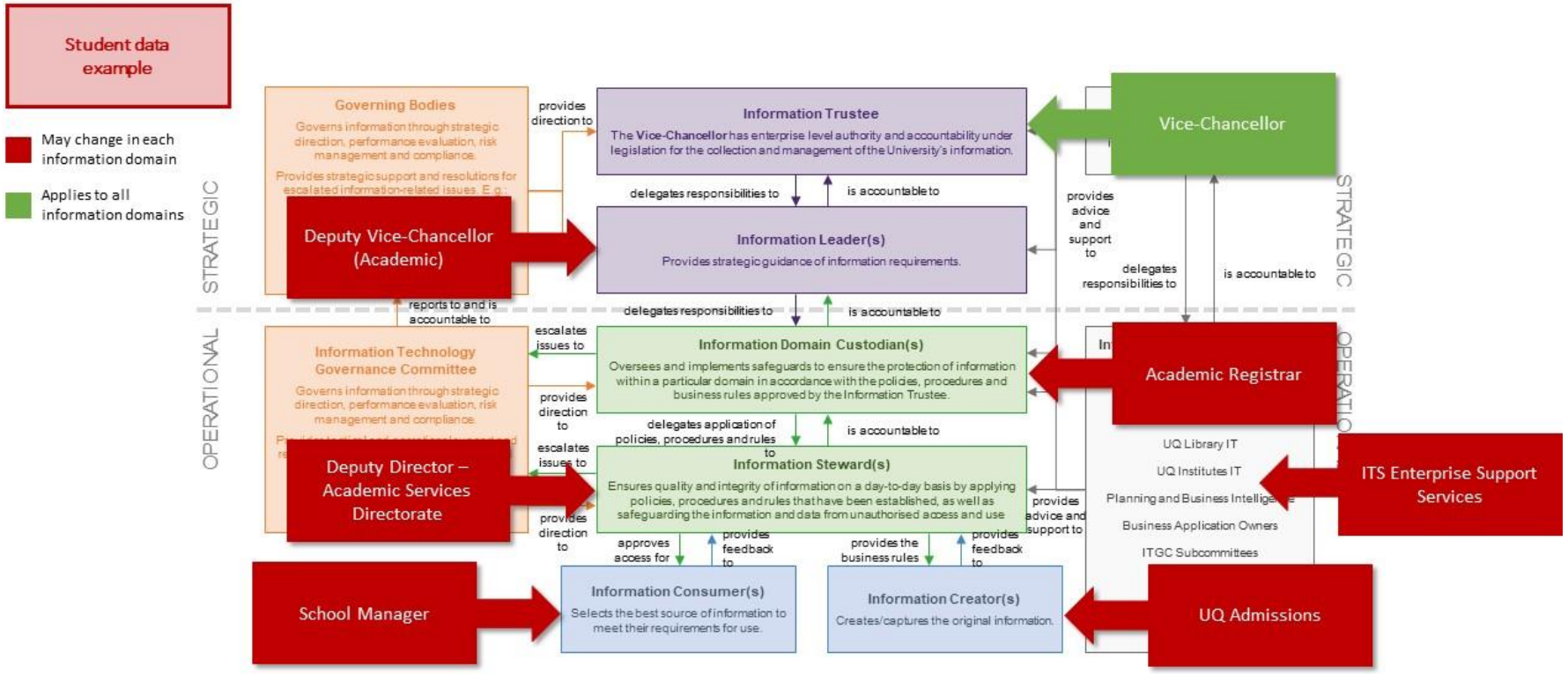
Business intelligence and reporting	• Practices for analysing information to optimise business decisions and performance. • Practices for ensuring that the information generated through business intelligence activities are retained, applied and fed back into business process and data quality improvement activities.
Data engineering	• Processes for preparing data for analytical or operational uses.
Data analytics	• Activities including the discovery, interpretation, and communication of meaningful patterns in data; and the process of applying those patterns towards effective decision making.
Data science	• A multi-disciplinary field that uses scientific methods, processes, algorithms and systems to extract knowledge and insights from structured and unstructured data.

Table 9 - Insights management capabilities

Note: Significant interdependencies exist between all capabilities. A single business initiative could be informed by multiple or all capability areas.

Appendix A **Decision rights example**

Using the decision rights model described in section 4.2, an example is given below using student data.



Appendix B **Governance controls**

Governance controls as of April 2019.

Lifecycle phase	Governance control	Source
Create and capture	Full and accurate records of activities are captured with regards to any relevant policy, standards and guidelines. Records providing evidence of the University activities are kept in accordance with legislation, policies and standards.	Public Records Act 2002
	A process is in place to ensure the appropriate collection, storage, use, management and disclosure of records in possession of the University. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Information Privacy Act 2009
	A process is in place to ensure the relevance of information in the University's possession. Information governance roles and responsibilities are embedded across the University to support the management of broadcasted information.	Broadcasting Services Act 1992
	Information governance roles and responsibilities are embedded across the University to support the management of information and data for electronic purposes.	Electronic Transactions Act
	A process is in place to ensure the appropriate collection and management of personal information in possession of the University. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Privacy Act 1988
	Full and accurate records of activities are captured with regards to any relevant policy, standards and guidelines. Records providing evidence of the University activities are kept in accordance with legislation, policies and standards.	Education Services for Overseas Students Act 2000
	Full and accurate records of students are captured with regards to any relevant policy, standards and guidelines.	Education Services for Overseas Students Regulations 2001

Lifecycle phase	Governance control	Source
	Full and accurate records are created with regards to any relevant policy, standards and guidelines. Records providing evidence of the University activities are kept in accordance with legislation, policies and standards.	Records Governance Policy
	A process is in place for the identification of records in possession of the University. The University staff are aware of their roles and responsibilities in the management of records in the information asset register.	Information Asset Custodianship Policy
	A process is in place for the description and classification of metadata information in possession of the University.	Metadata (IS34)
Store, classify and secure	Information governance roles and responsibilities are embedded across the University to support the management of information and data for electronic purposes.	Electronic Transactions Act
	A process is in place to ensure the appropriate use and disclosure of personal information in possession of the University. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Privacy Act 1988
	Full and accurate records of activities are captured with regards to any relevant policy, standards and guidelines. Records providing evidence of the University activities are kept in accordance with legislation, policies and standards.	Education Services for Overseas Students Act 2000
	A process is in place to ensure the appropriate storage of records in possession of the University. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Information Privacy Act 2009
Manage and maintain	A process is in place for the safe keeping, proper preservation and return of records in possession of the University. The University staff are aware of their roles and responsibilities in ensuring the safe keeping, proper preservation and return of records in possession of the University.	Public Records Act 2002
	Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Public Records Act 2002

Lifecycle phase	Governance control	Source
	A process is in place to ensure the safe custody and preservation of records in the University's possession.	Public Records Act 2002
	A process is in place to ensure the safe custody and preservation of protected information in the University's possession.	University of Queensland Act 1998
	Information governance roles and responsibilities are embedded across the University to support the access of information and data.	Information Privacy Act 2009
	A process is in place to ensure the appropriate management of records in possession of the University.	Information Privacy Act 2009
	Full and accurate records of activities are captured with regards to any relevant policy, standards and guidelines. Records providing evidence of the University activities are kept in accordance with legislation, policies and standards.	Right to Information Act 2009
	Full and accurate records of activities are captured with regards to any relevant policy, standards and guidelines. Records providing evidence of the University activities are kept in accordance with legislation, policies and standards.	Telecommunications (Interception and Access) Act 1979
	Records providing evidence of the University activities are kept in accordance with legislation, policies and standards and are available for access when required by law.	Cybercrime Act 2001
	A process is in place to ensure the relevance of information in the University's possession. Information governance roles and responsibilities are embedded across the University to support the management of broadcasted information.	Public Records Act 2002
	A process is in place to ensure the protection and management of intellectual property in the University's possession. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Copyright Act 1968

Lifecycle phase	Governance control	Source
	A process is in place to ensure the appropriate management of personal information in possession of the University. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Privacy Act 1988
	The University staff are aware of their roles and responsibilities in the management of records in possession of the University.	Records Governance Policy
	Information governance policies are consistent with broader agency frameworks and are embedded across the University to support the management of information and data.	Records Governance Policy
	A process is in place for the management of high-risk records in possession of the University.	Records Governance Policy
	A process is in place to ensure the appropriate management of records in possession of the University. Information governance policies are embedded across the University to support the management of information and data.	Information Governance Policy
	The University staff are aware of their roles and responsibilities in the management of records in possession of the University.	Information Asset Custodianship Policy
	A process is in place for the management of metadata information in possession of the University. Records providing evidence of the University activities are kept in accordance with policies and standards.	Metadata (IS34)
	A process is in place for participation in whole-of-government metadata consolidation initiatives.	Metadata (IS34)
	Full and accurate records of activities are created and maintained in the Provider Registration and International Student Management System (PRISMS) database.	National Code of Practice for Providers of Education and Training to Overseas Students 2018
	Records providing evidence of the University activities are kept in accordance with this policy. Activities are reported to the ESOS agency for the University, and have up-to-date information on specific aspects of the registered provider's operations and any registered courses.	National Code of Practice for Providers of Education and

Lifecycle phase	Governance control	Source
		Training to Overseas Students 2018
	An ISMS must be implemented and operated to ensure the protection of all information, application and technology assets.	Information security policy (IS18:2018)
	IT assets must be classified in accordance with the QGISCF. All information transmitted over data communications networks must be secured in line with the Network transmission security assurance framework (NTSAF). All services requiring user authentication must meet the requirements of the Queensland Government Authentication Framework (QGAF). We must implement the Australian Signals Directorate (ASD) “Essential Eight” Strategies to Mitigate Cyber Security Incidents.	Information security policy (IS18:2018)
Share and reuse	A process is in place to ensure the appropriate access to the records in possession of the University. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Public Records Act 2002
	A process is in place to ensure the safe custody and preservation of records in the University's possession.	Public Records Act 2002
	The University staff are aware of their roles and responsibilities when identifying, capturing and managing information.	Public Records Act 2002
	The University staff are aware of their roles and responsibilities when acquiring and using information.	University of Queensland Act 1998

Lifecycle phase	Governance control	Source
	A process is in place for the proper use of records in possession of the University. The University staff are aware of their roles and responsibilities in ensuring the proper use of records in possession of the University.	Information Privacy Act 2009
	Information governance roles and responsibilities are embedded across the University regarding the use of intercepted information and data.	Telecommunications (Interception and Access) Act 1979
	A process is in place for the relevance of information for commercial electronic messages sent by the University.	Spam Act 2003
	The University staff are aware of their roles and responsibilities when using information for electronic messaging.	Spam Act 2003
	Full and accurate records of activities are captured with regards to any relevant policy, standards and guidelines. Records providing evidence of the University activities are kept in accordance with legislation, policies and standards.	Evidence Act 1995
	A process is in place for the use of copyright literary works in possession of the University. The University staff are aware of their roles and responsibilities in ensuring the management of intellectual property in possession of the University.	Copyright Act 1968
	A process is in place to ensure the appropriate storage of personal information in possession of the University. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Privacy Act 1988
	Full and accurate records of activities are captured with regards to any relevant policy, standards and guidelines. Records providing evidence of the University activities are kept in accordance with legislation, policies and standards.	Education Services for Overseas Students Act 2000

Lifecycle phase	Governance control	Source
	A process is in place to ensure the protection and management of information in the University's possession. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Public Interest Disclosure Act 2013
Retain and archive	A process is in place to ensure the protection and management of information in the University's possession. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Public Interest Disclosure Act 2013
	A process is in place for the use of records in possession of the University.	Records Governance Policy
Dispose and destroy	Retention and disposal of information is managed in accordance with Queensland State Archives defined periods and the University's policies.	Public Records Act 2002
	A process is in place to ensure the appropriate access to the records in possession of the University. Information governance roles and responsibilities are embedded across the University to support the management of information and data.	Public Records Act 2002
	Information governance roles and responsibilities are embedded across the University to support the disposal of information and data.	Information Privacy Act 2009
	A process is in place to ensure the appropriate disposal and disclosure of records in possession of the University. Information governance roles and responsibilities are embedded across the University to support the disposal and disclosure of information and data.	Information Privacy Act 2009
	Information governance roles and responsibilities are embedded across the University to support the disposal of intercepted information and data.	Telecommunications (Interception and Access) Act 1979
	A planned and authorised process is in place for the disposal of records in possession of the University.	Records Governance Policy

Table 10 - Governance controls

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Contact details

Data Strategy and Governance
T +61 7 **3346 6881**
E datagovernance@uq.edu.au
W data.uq.edu.au

CRICOS Provider Number 00025B