GRIFFITH UNIVERSITY

Framework

Information Governance and Management

1.0 Purpose

This Information Governance and Management Framework (the Framework) and related policies support a consistent enterprise approach to information governance and information management across the University. The Framework outlines the University's obligations across the information life cycle and describes the governance and management structures.

2.0 Scope

This framework applies to staff, University Council members, University associates, Griffith controlled entities, and all persons conducting business or activities on behalf of the University, including whether as a visitor, adjunct appointee, service provider, contractor or volunteer participating in University business where they manage, create or use Griffith information or are authorised to access institutional data or information on behalf of the University. This framework does not apply to students.

Information-related roles specified in this framework hold additional responsibilities to ensure the safeguarding of availability, integrity and confidentiality of information assets commensurate with their classification.

This framework covers information resources hosted both on University premises and externally.

3.0 Framework

3.1 Information Approach

Griffith University is committed to appropriately managing all forms of information that it creates and holds to ensure that the right information is available to the right person, in the right format, at the right time. To achieve this, controls must be asserted over the University's information assets with the support of clear and effective information governance practices.

This framework supports the University's strategic vision by building an information-aware culture and delivering foundational capabilities and ways of working that leverage data and information as strategic assets, and to derive insights that inform decision making.

The University's approach for information governance and management is that:

- Information is managed in line with external statutory and internal administrative obligations.
- Information management supports and aligns with strategic objectives and organisational drivers.
- Custodianship and stewardship of information is improved through defined roles.
- Information is used and valued as an operational and strategic asset.
- Information is managed according to its purpose and associated risk profile.
- Appropriate controls are in place to secure information according to its value and risk profile.

This approach will enable effective: planning and decision making; performance management; information creation and collaboration; information discovery, access and distribution; information quality and integrity; regulatory compliance; and communication within the University and between the University and its stakeholders.

3.2 Information Domains

The University's data and information is notionally organised into high level domains and sub-domains. These domains are defined as:

- **Scholarly Information**: Research outputs and the learning and teaching materials created.
- **Managing Scholarship**: Research and learning and teaching management information.
- **Supporting University Business**: Information and data that supports University business functions.

An Information Leader will typically be assigned to an Information Domain and Information Custodians to the sub-domains.

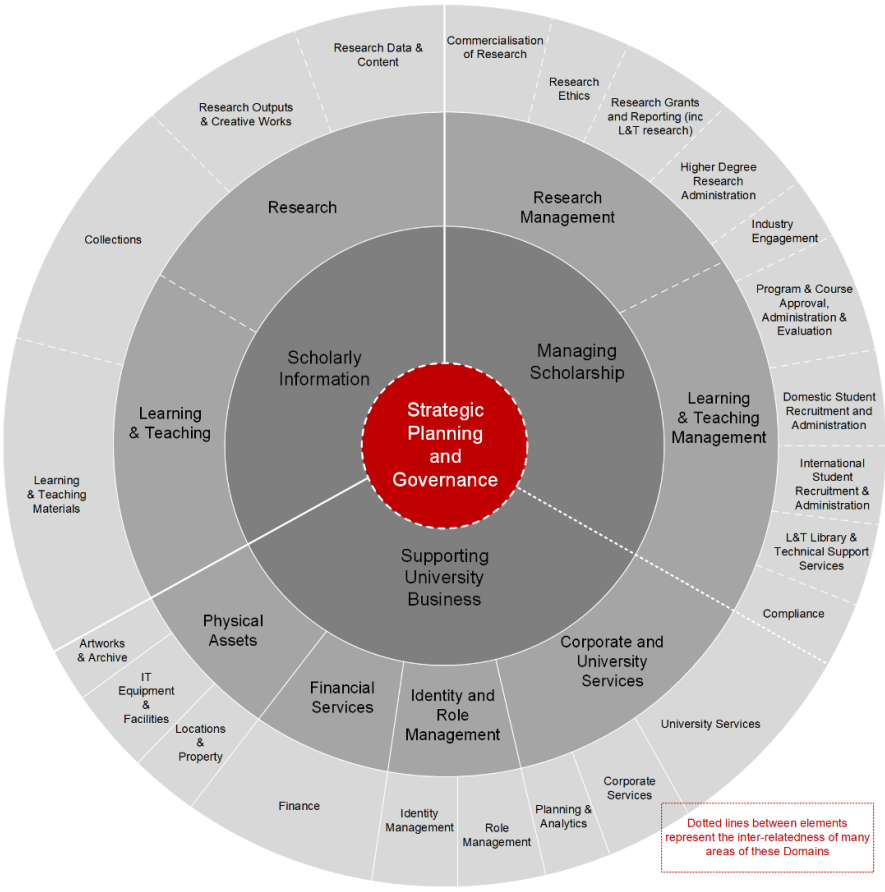

Figure 1: Griffith University Information Domain and Sub-Domains

4.0 Information Governance

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

4.1 Governance Context

Effective information governance underpins delivery of any data-related strategic initiatives.

4.2 Decision Rights

Clearly defined decision rights support effective information governance and efficient decision-making for information and data management. The 'Decision rights model for information governance' outlines the decision-making hierarchy across strategic and operational areas of responsibility (see Figure 2). It should be read in conjunction with information-related roles and responsibilities (see section 4.3 of this Framework).

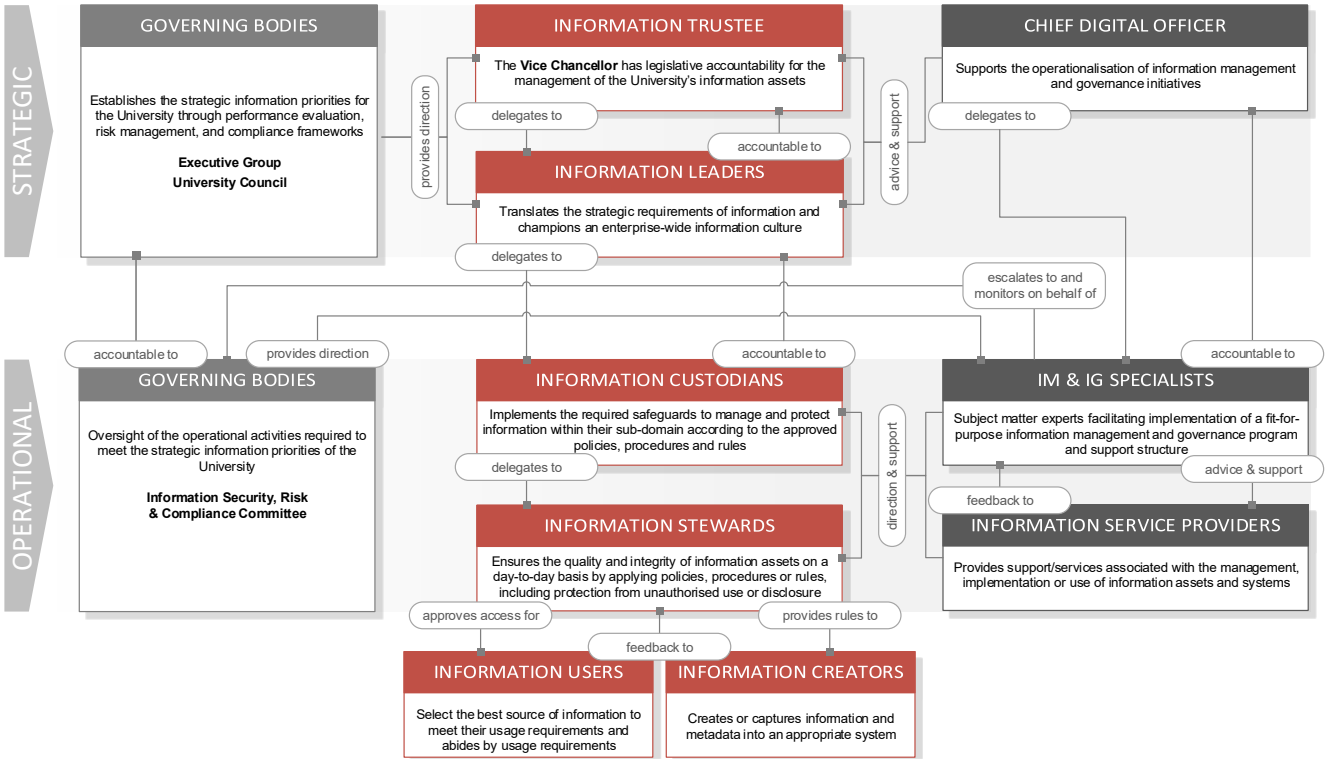

Figure 2: Decision rights model for information governance

4.3 Roles and Responsibilities

The following roles and responsibilities are required for the effective collection, management and use of University information.

ROLE	RESPONSIBILITY
Information Trustee	▪ Enterprise-wide authority and accountability for the collection and management of the University's information.
Information Leader	▪ Strategic guidance regarding information requirements. ▪ Executive-level champions of the University's information culture.
Governing Bodies	▪ Remain informed and supportive of information governance and management initiatives
Chief Digital Officer	▪ Oversee a framework for the management of information risk and the University's information management and cybersecurity programs.
Information Management & Governance Specialists	▪ Operationally implement information management and information governance programs.
Information Service Providers	▪ Support embedding information governance controls into systems and practices.
Information Custodian	▪ Define and implement safeguards to ensure the protection of information in their sub-domain.
Information Steward	▪ Day-to-day management of the integrity and quality of information assets and protection against unauthorised use.
Information Creator	▪ Capture or create information.
Information User	▪ Use the best source of information. ▪ Report incidents of University information being at risk.

The following is an example of roles mapped to a Human Resources data set.

ROLE	POSITION
Information Trustee	▪ Vice Chancellor
Information Leader	▪ Chief Operating Officer
Information Custodian	▪ Human Resources Director
Information Steward	▪ Senior Manager, People Services
Information Creator	▪ HR staff (depending on data input methods)
Information User	▪ Staff with relevant access permissions ▪ Planning & Analytics

ROLE	DESCRIPTION	ACCOUNTABLE FOR	RESPONSIBLE FOR
Information Trustee	Has University-wide authority and accountability under legislation for the compliant collection and management of the University's information and may delegate these responsibilities to other roles. Griffith's Information Trustee (or Information Owner) is the Vice Chancellor.	▪ compliant collection and management of the University's information in accordance with relevant legislative, regulatory and policy obligations.	▪ 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 appropriately delegated ▪ approving or endorsing University-wide policies, procedures and rules associated with governing and managing information (within the delegation responsibilities of the Vice Chancellor or University Council) ▪ supporting business cases relating to information management investments aligned to strategy ▪ assigning Information Leaders to the University's high-level information domains.
Information Leader	Provides strategic guidance regarding information requirements usually within a high-level information domain.		▪ championing information governance and information-related initiatives by 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 their information domain.
Governing Bodies (refer Figure 2: Decision rights model for information governance)	Be informed of information governance, information management and information security initiatives commensurate	▪ resolving issues escalated via a data remediation process.	•

ROLE	DESCRIPTION	ACCOUNTABLE FOR	RESPONSIBLE FOR
	with their terms of reference or constitution.		
Chief Digital Officer (CDO)	Managing the technical and specialist teams relevant to information governance and quality issues	▪ developing and maintaining the information management priorities ▪ understanding the data security needs and implementing appropriate controls ▪ developing information policies, standards and procedures	▪ interpreting the business and information needs, and strategic goals of the University and translating them into Information and Communication Technology (ICT) initiatives that deliver or support maintaining valued information assets ▪ supporting the Information Trustee and Information Leaders in determining the strategic direction for information management and governance and supporting related ICT initiatives ▪ ensuring that Digital Solutions' Information Service Providers are adequately resourced ▪ ensuring that alleged breaches of information security and information management protocols are investigated ▪ ensuring that appropriate mitigation and response measures are taken following investigations of misuse/breaches ▪ ensuring that the Information Management Policy and supporting procedures are maintained and operationally enforced. The CDO may delegate responsibilities to relevant IT Directors and Information Management & Governance Specialists.
Information Management and Information Governance Specialists	Primarily located in the Digital Solutions teams of Information Management and Solutions, Digital Trust, and IT Governance,		▪ development and maintenance of the information governance and management framework (this document) and related policies and procedures ▪ interpreting legislation and regulatory requirements to ensure the University's information management and information security policies and procedures align to comply

ROLE	DESCRIPTION	ACCOUNTABLE FOR	RESPONSIBLE FOR
	Risk, Compliance and Continuity.		▪ embedding risk management into information, data and IT governance artefacts and translating them into strategies to reduce risk. ▪ planning and managing compliance monitoring and reporting activities as they relate to information and data ▪ ensuring that information assets are managed throughout their lifecycle commensurate with the identified risk and value ▪ developing and deploying work practices that facilitate an information-aware culture
Information Service Providers Solutions Architects and Project Managers (in the solution design phase) Business system administrators/product service managers Infrastructure support teams Committees such as Solution Architecture Board (SAB) and Information Technology Advisory Board (ITAB)	Technical teams that administer/support University information-related ICT solutions and information systems. They provide support for embedding the required governance controls and processes.		▪ planning and managing compliance monitoring and reporting activities as they relate to information and data within their area of expertise ▪ ensuring that information assets within business applications in their area of expertise are managed throughout their lifecycle commensurate with the identified risk and value ▪ ensuring appropriate technical and personnel security measures are in place commensurate with the risk of the information contained in business applications in their area of expertise ▪ designing solutions which meet the information needs of the University.

ROLE	DESCRIPTION	ACCOUNTABLE FOR	RESPONSIBLE FOR
Information Custodians	Define and implement safeguards to ensure the protection of information in their information sub-domain in accordance with approved policies, procedures and rules.		<u>Within their sub-domain:</u> ▪ defining the 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 records management practices are followed throughout the information lifecycle ▪ managing and maintaining information and its metadata, to ensure that discovery is possible ▪ escalating information-related risks through the University's risk management processes, and managing that risk accordingly ▪ assuring the quality and integrity of information ▪ monitoring and responding to performance measures ▪ approving and documenting the release of information to external parties based on approved criteria ▪ ensuring that disposal of information assets/records is undertaken in accordance with University policies and procedures ▪ assigning and supporting Information Stewards to oversee day-to-day information asset management.
Information Stewards	Attend to the quality, integrity and use of an information asset on a day-to-day basis and may manage multiple information assets.		▪ monitoring and continuously improving the quality of an information asset ▪ the application and compliance with relevant legal, policy and standards requirements ▪ the application of security, confidentiality and privacy requirements

ROLE	DESCRIPTION	ACCOUNTABLE FOR	RESPONSIBLE FOR
			▪ ensuring information is consistently and accurately captured in the approved information system (in conjunction with Information Creators) ▪ providing advice to Information Users on the proper use and interpretation of information ▪ reviewing and approving (or rejecting) internal requests for access to information assets/data ▪ reviewing and submitting disposal requests of information assets/records. ▪ arranging training for current and potential users before granting application(s)/systems (and by extension information and data) access.
Information Creator	Capture or create information as defined by the Information Custodian. Most staff will be Information Creators.		▪ accurately capturing information/data in line with legislation, policy and standards ▪ complying with information governance policies, procedures, processes and rules ▪ seeking advice on information requirements and providing feedback to the relevant Information Steward.
Information Users	Select the best source of information to meet their use-case and define the criteria of what makes information fit-for-purpose. All staff will be Information Users.		▪ only accessing and using information assets as approved ▪ using the University's information assets in line with all relevant information-related legislation, policies, procedures and processes ▪ using the University's information assets ethically and securely, respecting confidentiality and privacy ▪ reporting any actual or suspected incidents of University information at risk of breach.

4.4 Governance Controls

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

The level of control applied to the information will be commensurate with the value of the information asset and the risks associated with its collection, use and exposure. Enterprise level controls are applicable to all University information, and particular business level controls apply to information sub-domains where specified.

Processes to enforce the controls may be technology-enabled/automated or manual.

See Appendix A: Broad governance controls mapped to information lifecycle and legislative requirements.

5.0 Information Management

5.1 Information Management Principles

Transparent	▪ Information assets are discoverable across the University by those with legitimate need
Trustworthy	▪ Information assets are accurate, up-to-date and complete. ▪ Systems protect information assets from unauthorised alteration, deletion or misuse.
Secure	▪ Information processes reflect best practice standards and comply with relevant legislation and regulatory requirements.
Usable	▪ Information assets are ready for re-use, interoperable across the University, and available and usable for as long as needed.
Valued	▪ Staff understand and appreciate the value of information as an asset
Managed	▪ Governance mechanisms ensure that information management decisions are made with integrity, accountability and transparency, and deliver fit-for-purpose business outcomes.

The Information Management Principles are supported by active management of information assets through their lifecycle.

5.2 Information Lifecycle Management

Information lifecycle management is the consistent management of information from creation to final disposition. It comprises policies, processes and technologies with assigned roles and responsibilities for effective information management and improved control over the information lifespan.

Information lifecycle management activities are **coordinated** by Information Management & Solutions within Digital Solutions to ensure that information is:

- created, captured and classified adequately
- secured and stored appropriately

- managed and maintained compliantly
- shared and reused and discoverable where appropriate
- retained and archived for the minimum period commensurate with business needs
- disposed of and destroyed correctly.

6.0 Definitions

For the purposes of this policy and related policy documents, the following definitions apply:

A **Critical Information Asset** is an unstructured or structured information asset, which if compromised, degraded, rendered unavailable for an extended period or destroyed, would have a moderate to severe impact (as defined in the Enterprise Risk Management Framework) on the viability and sustainability of the University.

The terms **data and information** are used interchangeably. This scope of this definition includes both structured and unstructured data, meaning data in a structured format such as databases, system and log files; as well as unstructured data which can include a range of sources such as various document types, blogs, emails, social media etc.

An **Information Asset** is an identifiable collection of information, defined and managed as a single unit so it can be understood, shared, protected and utilised effectively. It is recognised as having value for the purpose of enabling the University to perform its business functions and supporting processes.

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 throughout their lifecycle.

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.

Information Security Classification is a process where the creator of information assesses the sensitivity and importance of the information and assigns a label to the information so that it can be managed or stored with consideration to its sensitivity and importance.

Protective Marking is a physical or electronic label attached to information to indicate the Security Classification that is assigned.

University information is any information (irrespective of format) created, received or managed by Griffith University staff, associates, contractors, volunteers or students in connection with their employment, business dealings, research or studies at the University.

7.0 Information

Title	Information Governance and Management Framework
Document number	2025/0001039

Purpose	The Information Governance and Management Framework (the Framework) and related policies support a consistent enterprise approach to information governance and information management across the University. The Framework outlines the University's obligations across the information lifecycle and describes the governance and management structures.
Audience	Staff
Category	Operational
Subcategory	Information Management
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal: 16: Peace, Justice and Strong Institutions
Approval date	1 May 2025
Effective date	1 May 2025
Review date	2030
Policy advisor	Head of Information Management and Solutions
Approving authority	Chief Digital Officer

8.0 Related Policy Documents and Supporting Documents

Legislation	**Federal Acts** *Broadcasting Services Act 1992* *Copyright Act 1968* *Cybercrime Act 2001* *Education Services for Overseas Students Act 2000* *Privacy Act 1988* *Spam Act 2003* *Telecommunications (Interception and Access) Act 1979*

	Telecommunications Act 1997 **State Acts (Queensland)** *Evidence Act 1977* *Electronic Transactions (Queensland) Act 2001* *Griffith University Act 1998* *Information Privacy Act 2009* *Public Interest Disclosure Act 2010* *Public Records Act 2023* *Right to Information Act 2009* **Federal Policies** Australian Code for the Care and Use of Animals for Scientific Purposes, 2013 Australian Code for the Responsible Conduct of Research, 2018 National Code of Practice for Providers of Education and Training to Overseas Students 2018 **State Policies (Queensland)** General Retention and Disposal Schedule (GRDS) Information Standard: Information Security IS18 Records Governance Policy University Sector Retention and Disposal Schedule (QDAN 601) **International** Aspects of various international regulations may apply to some operations of the University e.g.: General Data Protection Regulation (GDPR) or California Consumer Privacy Act or similar.
Policy	Information Management Policy Information Security Policy
Procedures	Information Security Classification Procedure Information Security Procedure IT Code of Practice
Local Protocol	N/A
Forms	N/A