Data Governance Policy

Section 1 - Purpose

(1) The purpose of this Policy is to establish a framework of principles for governing the University's data as a strategic asset, enabling its responsible use while protecting the University and its community. This Policy complements existing policies on information classification, privacy, cybersecurity and Research Data management, and defines the framework for governing University Data.

Background

(2) This Policy applies to all types of data created, collected, or used in the University and its controlled entities. For clarity, three main categories of data are recognised:

a. Enterprise Data is the University's official and authoritative data that is exchanged between organisational units, used to perform business process activities, or required for retrieval, reporting, and institutional accountability. Enterprise Data support core functions such as education, research management, finance, human resources, and administration, regardless of physical storage location. Enterprise Data includes Enterprise Data Products (curated datasets, dashboards, reports, analytical models, and AI models) certified for authorised consumption.
    i. Enterprise Data does not include personal notes, working drafts, informal communications (e.g., chat messages, ad hoc emails), or data used solely within a single organisational unit for immediate purposes, unless such materials are formally designated as official records or required to be retained under legislation, regulation, or University policy.
b. Research Data is defined in the Research Data Management Policy and includes, but is not limited to, primary materials or information held in any digital format or media, or anything that can be digitised, on which an argument, theory, test or hypothesis, or another research output is based.
c. Local Data is created, collected, and managed by individuals, teams, or organisational units for purposes specific to their immediate operational or analytical needs within that unit. Local Data commonly takes the form of documents, emails, spreadsheets, small databases, or extracts of Enterprise Data sources stored on devices, departmental drives, SharePoint, OneDrive, or other platforms. Unlike Enterprise Data, Local Data is not authoritative or centrally governed but must still be managed responsibly, according to the principles described below, particularly where it contains sensitive, confidential, or regulated information.

Scope

(3) This Policy applies to:

a. all employees of the University and its controlled entities;
b. all students of the University including former students;
c. all University researchers and Graduate Research Academy (GRA) students; and
d. any person who handles University data for or on behalf of the University or its controlled entities, including contractors, agents, visitors, honorary, clinical or adjunct appointees and consultants of the University.

(4) This Policy applies to all types of digital data created, collected, or used by or on behalf of the University.

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.

(5) The Policy structure reflects different governance requirements:

a. Parts A and B establish principles and user obligations that apply to all University data including Local Data;
b. Parts C and D establish specific governance provisions for Enterprise Data and Enterprise Data Products;
c. Parts E and F establish specific governance provisions for Research Data; and
d. where Local Data becomes critical to business processes or poses institutional risk, individuals and teams managing such data must work with Data Stewards to assess whether it should be elevated to Enterprise Data status with appropriate governance controls.

(6) This Policy works in conjunction with the following University policies:

a. Privacy Policy – specific provisions to ensure protection of the personal data;
b. Cyber Security Policy – specific provisions to ensure security of all types of data;
c. Data Breach Policy – specific provisions to meet obligations in event data is breached;
d. Responsible and Ethical Use of Artificial Intelligence Policy – specific provisions to ensure data used for artificial intelligence is ethical;
e. Glossary Policy – specific provisions for how business definitions are managed to provide clarity on how Enterprise Data should be interpreted and presented;
f. Records and Information Management Policy - specific provisions to ensure University's Records and information system complies with legislative requirements;
g. Research Data Management Policy; and
h. any relevant policies specific to individual controlled entities.

(7) This Policy also works in conjunction with specific procedures and guidelines that provide detailed requirements on how key elements of data governance are applied and are listed in the appropriate sections below.

Section 2 - Policy

Part A - Data Governance Principles

(8) The following principles underpin the University's approach to data governance and are expected to be applied to guide decision-making about data management across all contexts:

a. Accountability and Stewardship - All University data must have a designated Data Owner who is accountable for ensuring appropriate governance, quality, and compliance. Data is managed as a shared institutional asset requiring responsible stewardship;
b. Privacy and Confidentiality - Personal and Sensitive data and information must be protected throughout its lifecycle in accordance with privacy legislation and ethical obligations;
c. Transparency and Trustworthiness - The University is transparent about how data is used, governed, and protected, building trust within the University community and with external stakeholders;
d. Ethical and Responsible Use - Data is used ethically, responsibly, and in accordance with its intended and approved purposes, including compliance with research ethics requirements;
e. Security and Protection - Data is protected from loss, unauthorised access, misuse, and disclosure through appropriate security measures proportionate to its sensitivity and value;
f. Quality and Fitness for Purpose - Data quality is actively managed to ensure it is accurate, complete, and fit for its intended purposes;
g. Minimisation - Data is shared as openly as possible but restricted where necessary to protect privacy, security, ethical, legal, or proprietary interests. Access is granted based on legitimate need, and users must collect,

access, and use only the minimum data necessary for their authorised purpose; and

h. Continuous Improvement - The University is committed to enhancing data governance maturity through regular review, audit, and compliance reporting.

Part B - Obligations for All Users of University Data

(9) All individuals who create, collect, access or use University data must:

a. comply with the Privacy Policy when handling personal or sensitive data;
b. retain data only for as long as necessary to fulfil the purposes for which it was collected and abide by the provisions of the Records and Information Management Policy and Retention and Disposal Procedure;
c. ensure that data under their control are managed in a manner that is compliant with this Policy, and that any new data they create, collect, or materially transform has a designated Data Owner who is accountable for its ongoing governance;
d. be transparent about how the data is being used and take steps to ensure they are being managed appropriately for the stated purpose;
e. handle data ethically and responsibly and in accordance with the Research Data Management Policy, the Research Data Management Procedure and the Responsible and Ethical Use of Artificial Intelligence Policy as applicable;
f. classify data and manage it in accordance with the Information Classification and Handling Procedure and, where applicable, the Research Data Sensitivity, Security and Storage Guideline;
g. ensure that the quality of the data is fit for purpose;
h. store data in University approved systems where it is protected from loss, unauthorised access, use and disclosure and abide by the provisions of the Cyber Security Policy and the Data Breach Policy;
i. request, access, use and share only the minimum data necessary for the authorised purpose, recognising that data should be shared as openly as possible but restricted where necessary to protect privacy, security, ethical, legal, and proprietary interests; and
j. conduct or support the conduct of periodic audits of data under their control to ensure on-going compliance with this Policy and all related policies.

Part C - Enterprise Data Governance Structure

(10) The Vice-Chancellor will nominate a member of the Executive Group as the Enterprise Data Governance Executive Sponsor to be accountable for ensuring the implementation of, and compliance with, this Policy.

(11) The Data Governance Executive Sponsor will establish Domain-specific Data Governance Groups that will drive the implementation of this Policy and associated procedures to ensure compliance across the University and its controlled entities from a business perspective.

(12) The Data Governance Groups will operate within the existing management structures of the University and its controlled entities.

(13) A Data Design Authority (DDA) will be established to operate under the governance of the IT Architecture Review Board (ARB) and will drive the implementation of this Policy and associated procedures from an enterprise IT architecture and design perspective.

Part D - Enterprise Data Governance Roles and Responsibilities

(14) The Enterprise Data Governance Executive Sponsor:

a. will direct Domain Data Governance Groups, Data Owners, and Data Custodians to provide status reports according to the requirements of this Policy; and
b. will provide status reports to the governing bodies of the University as required.

(15) The Chief Data Officer is responsible for leading and coordinating the definition, implementation, and continuous improvement of this Policy and its associated procedures, standards, and guidelines in support of the Data Governance Executive Sponsor.

(16) The Chief Information and Digital Officer (CIDO) will support the Executive Sponsor with the management, operation, and security of all infrastructure and applications that hold Enterprise Data, and the implementation of this Policy and associated procedures from a technology perspective.

(17) Domain Data Governance Groups:

a. are established by the Data Governance Executive Sponsor and will cover all Domains of the University and controlled entities, to ensure all Enterprise Data is included;
b. operate under the authority of a nominated management committee that will provide oversight and set strategic direction;
c. support the Data Governance Executive Sponsor with compliance reporting for their Domain as required and must:
    i. develop and maintain Domain-specific data strategies aligned with the strategic priorities of the Domain;
    ii. assign Data Owners and Data Stewards for all Enterprise Data;
    iii. approve and provide oversight of the use of Enterprise Data for analytics and Artificial Intelligence (AI) ensuring alignment with Domain-specific strategic priorities, compliance with relevant policies, procedures and guidelines and ensure that Enterprise Data risk is documented, assessed, and managed in accordance with the Risk Management Policy and associated frameworks and processes;
    iv. establish lifecycle management principles including retention and disposal considerations for Enterprise Data;
    v. establish Access Management principles for Enterprise Data;
    vi. assign librarians for Domain-specific business terms and provide oversight of the development of the Glossary of associated business definitions;
    vii. provide oversight of the certification of Enterprise Data Products;
    viii. provide oversight of data quality management of Enterprise Data;
    ix. establish criteria and processes for assessing when Local Data should be elevated to Enterprise Data status, including consideration of cross-organisational use, institutional risk, regulatory requirements, and business criticality;
    x. maintain oversight of Local Data that has been identified as critical to business processes within their Domain, ensuring appropriate risk mitigation strategies are in place even where full Enterprise Data governance is not yet applied;
    xi. lead policy reviews related to Data Governance and standard settings within their Domains; and
    xii. drive data literacy, adoption, and training initiatives.

(18) Data Owners:

a. are assigned by the Domain Data Governance Groups as accountable for applying the provisions of this Policy and associated procedures to designated Enterprise Data assets and must:
    i. approve classification;
    ii. define the purpose of and approve usage;

iii. delegate a Data Steward to manage day-to-day governance activities;
iv. define clear rules for Access Management and monitor compliance;
v. ensure adherence to agreed Data Lifecycle principles including retention and disposal;
vi. ensure certification of Enterprise Data Products;
vii. ensure effective management of data quality;
viii. ensure compliance with privacy, ethical, legal, regulatory, and information security obligations; and
ix. assess Local Data assets identified by Data Stewards as potentially meeting Enterprise Data criteria, and where appropriate, approve the elevation of such data to Enterprise Data status with associated governance controls, including assignment of necessary resources and integration into Domain governance structures.

(19) Data Stewards:

a. are delegated by Data Owners as the business subject matter experts responsible for day-to-day governance of designated Enterprise Data assets and must:
    i. act as expert advisors to the Data Owners on matters related to Enterprise Data Governance;
    ii. lead good data management practice;
    iii. work with users and Data Custodians to resolve data quality issues;
    iv. ensure management of business Metadata;
    v. ensure effective data quality monitoring controls;
    vi. support Access Management approvals and reviews;
    vii. identify Local Data assets within their Domain that have become critical to business processes, assess associated risks, and recommend to Data Owners whether such assets should be elevated to Enterprise Data status with appropriate governance controls; and
    viii. maintain awareness of secondary data uses being created from Enterprise Data at the local level, and where such uses represent risk or could benefit from improved data quality, work with local data creators to implement appropriate controls or integrate data into Enterprise Data governance.

(20) The Data Design Authority (DDA):

a. is established by the Chief Information and Digital Officer (CIDO) and Chief Data Officer (CDO) and will operate as a technical advisory group under the IT Architecture Review Board (ARB);
b. is accountable for ensuring the IT Enterprise Data Platform is compliant with the Data Governance Policy and procedures; and must:
    i. assign Data Custodians for Enterprise Data;
    ii. own, maintain, and manage the Information Asset Register;
    iii. define guidelines, standards, and practices for the technical implementation of the requirements of this Policy and associated procedures; and
    iv. ensure all design activities relating to the Enterprise Data Platform comply with the agreed guidelines, standards and practices.

(21) Data Custodians:

a. are responsible technical experts for designated Enterprise Data assets and must:
    i. ensure data is properly secured, classified, and accessed according to this Policy and associated procedures;
    ii. manage the lifecycle of data from creation to disposal;

iii. support and maintain data quality, definitions, and Metadata;
iv. monitor and report on data usage, compliance, and governance adherence;
v. collaborate with Data Stewards to identify technical solutions that can bring critical Local Data under appropriate governance controls, including integration into Enterprise Data Platform where feasible; and
vi. collaborate with Data Stewards to resolve data issues and support governance initiatives.

Part E - Research Data Governance Structure

(22) The Vice-Chancellor will nominate a member of the Executive Group as the Research Data Governance Executive Sponsor to be accountable for ensuring the implementation of, and compliance with, this Policy.

(23) The Research Data Governance Executive Sponsor will establish the Research Data Governance (RDG) Group that will drive the implementation of this Policy and associated procedures to ensure compliance across the University and its controlled entities from a research perspective.

(24) The RDG Group will operate within the existing management structures of the University and its controlled entities.

Part F - Research Data Governance Roles and Responsibilities

(25) The Research Data Governance Executive Sponsor:

a. will direct the Research Data Governance (RDG) Groups and is accountable for the implementation of, and compliance with, the Data Governance Policy across all the University's research activities and controlled entities;
b. nominates the Chair of the RDG; and
c. will provide status reports to the governing bodies of the University as required.

(26) The Pro Vice-Chancellor, Research Services is responsible for leading and coordinating the definition, implementation, and continuous improvement of this Policy and its associated procedures, standards, and guidelines in support of the Research Data Governance Executive Sponsor.

(27) The Chief Information and Digital Officer (CIDO) will support the Research Data Governance Executive Sponsor with the management, operation, and security of the infrastructure, systems, platforms, and applications associated with Research Data, and the implementation of this Policy and related procedures from a technology perspective. The CIDO will also establish a Research Data Authority (RDA) to serve as a technical advisory group responsible for translating Research Data governance requirements into technical standards and ensuring compliance of Research Data infrastructure with those standards.

(28) The Research Data Governance (RDG) Group:

a. supports the Research Data Governance Executive Sponsor with implementation of this Policy and fostering responsible research across the University's research activities and controlled entities;
b. supports the implementation, review, and continued relevance of the Research Data Management Policy, ensuring that policy provisions are actionable and that support, infrastructure, and compliance measures are in place and resourced appropriately;
c. provides oversight and direction for the following institutional responsibilities:
    i. establishes and maintains good governance practices for responsible Research Data management;
    ii. identifies and ensures compliance with relevant laws, regulations, guidelines and policies related to the management of Research Data;

iii. develops and maintains the currency of the Research Data Management Policy;
iv. ensures the provision of ongoing training and education that promotes and supports responsible Research Data management;
v. supports the responsible dissemination of Research Data;
vi. ensures researchers have access to facilities for the safe and secure storage and management of Research Data, which, where possible and appropriate, enables access and reference to that Research Data by others;

d. provides guidance on the clarity of Research Data governance responsibilities across the Research Data lifecycle;
e. provides strategic direction and requirements for Research Data management capabilities, workflows, and sustainability to support responsible research conduct, and advises the RDA on data governance requirements that must be reflected in technical standards and infrastructure design;
f. identifies and escalates strategic IT risks related to Research Data governance to the CIDO, in consultation with the RDA where technical expertise is required; and
g. collaborates with the relevant Enterprise Domain Data Governance Groups to ensure seamless alignment on cross-domain matters, including, but not limited to, governance of research metadata when used for institutional reporting or research administration.

(29) The Research Data Authority (RDA):

a. is established by the Chief Information and Digital Officer (CIDO); and
b. is accountable for ensuring Research Data infrastructure is compliant with the Data Governance Policy and Research Data Management Policy, and must:
    i. define and maintain technical guidelines, standards, and practices for the implementation of Research Data governance requirements;
    ii. review and endorse technical solutions and platforms proposed for Research Data management to ensure compliance with agreed technical standards and data governance requirements;
    iii. collaborate with the RDG to ensure that the technical implementation of research data management standards, workflows, access controls, maintenance and oversight aligns with institutional data governance standards; and
    iv. provide technical guidance to the RDG on data governance matters requiring technical expertise, including the feasibility of developing and enhancing technical capabilities for governing research data, risk assessment, and relevant standards compliance.

(30) For other Research Data Governance Roles and Responsibilities refer to the Research Data Management Policy and the Research Data Management Procedure.

Section 3 - Procedures

(31) This Policy works in conjunction with the following Procedures:

a. Information Classification and Handling Procedure;
b. Retention and Disposal Procedure; and
c. Research Data Management Procedure.

Section 4 - Guidelines

(32) This Policy works in conjunction with the following Guidelines:

a. Research Data Sensitivity, Security and Storage Guideline.

Section 5 - Definitions

(33) The following specific definitions apply for the purpose of this policy:

a. Access Management means the security practice that regulates, controls, and monitors who can access a designated data asset. This is usually role-based as determined by defined access principles.
b. Data Governance refers to a framework that defines decision-making, roles, responsibilities, policies, procedures and standards for the effective management of University data.
c. Data Lifecycle refers to the progression of a data asset through various stages from creation or collection, through access and usage, to retention, archival or secure destruction/disposal.
d. A Domain is a defined area of organisational activity and accountability that represents a coherent set of related functions, processes, and data assets, aligned to the University's core purposes and operations. Domains provide a structured framework for assigning stewardship, governance responsibilities, and decision-making authority over data. Examples include (but are not limited to) Education, Research, Staff/Human Resources, and Finance. Each Domain is distinct in scope, while interconnected with other Domains through shared data and processes, and is governed to ensure consistency, integrity, and alignment with institutional objectives.
e. Enterprise Data Platform is the IT-managed environment for collecting, processing, and managing Enterprise Data to support data integration, operational reporting, and the development of strategic Enterprise Data Products.
f. Enterprise Data Product is a curated, purposefully designed data asset developed from Enterprise Data sources to support specific business needs, decision-making, or analytical purposes. Enterprise Data Products include datasets, dashboards, reports, analytical models, and AI models that are certified and made available for consumption by authorised users.
g. Information Asset Register is a comprehensive and centralised inventory of the University's key information assets, documenting ownership, classification, usage, retention.
h. Metadata is descriptive information about data that enables it to be discovered, accessed, and managed.

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.

Status and Details

Status	Current
Effective Date	20th February 2026
Review Date	20th February 2031
Approval Authority	Vice-Chancellor
Approval Date	20th February 2026
Expiry Date	Not Applicable
Responsible Executive	Jonathan Wylie Vice-President, Strategy, Planning and Performance +61 2 9850 7350
Responsible Officer	David Miller Chief Data Officer +612 9850 1624
Enquiries Contact	David Miller Chief Data Officer +612 9850 1624

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.