

Data Governance Policy

Section 1 - Key Information

Policy Type and Approval Body	Administrative - Vice-Chancellor
Accountable Executive - Policy	Chief Operating Officer
Responsible Manager - Policy	Chief Data and Analytics Officer (DDA)
Review Date	8 October 2029

Section 2 - Purpose

(1) Data Governance is the exercise of authority, control, and shared decision-making (planning, monitoring and enforcement) over the management of data assets.

(2) Institutional data is defined as data created, received, maintained and/or transmitted by the University. Institutional data is used for reporting and decision making. Examples include: enrolment data, financial data, staff data, course data and subject data.

(3) This Policy establishes the principles, roles and responsibilities required for institutional Data Governance to ensure the effective management of data.

Section 3 - Scope

(4) This Policy applies to:

- a. all institutional data; and
- b. students, staff, contractors, third-parties, CONAGOTHs (Consultants, Agency or Other) and other members of the University community who use or have access to the University's data.

(5) This Policy does not apply to:

- a. Research data as defined in [Research Data Management Policy](#); or
- b. Unstructured information assets, including documents, records, emails, and file-based content, which are governed under the [Records Management Policy](#).

Section 4 - Key Decisions

Key Decisions	Role
Approve data sets, business terms, access, quality rules, reference data and business entities	Data Custodians
Approve data classifications in terms of sensitivity and security, taking into account relevant legislation and privacy acts	Data Custodians

Key Decisions	Role
Prioritise enterprise data quality issues, score carding and monitoring	Data Governance Committee
Approve remediation actions for unresolved or escalated data quality issues	Data Governance Committee
Approve data sources for metadata scanning and profiling	Data Governance Committee

Section 5 - Policy Statement

(6) The University acknowledges the role of institutional data in achieving its strategic and operational objectives. The University applies the following fundamentals when governing institutional data:

- institutional data is an asset of the University;
- data is governed through defined roles and responsibilities;
- individuals are responsible for the data they collect and manage on behalf of the University;
- data must be of good quality e.g. accuracy, completeness, consistency, timeliness, validity and uniqueness, and managed consistently across its lifecycle;
- the management of institutional data must comply with applicable legislation and relevant policies; and
- institutional data is held securely and protected from unauthorised access, use and disclosure.

Section 6 - Procedures

Part A - Roles and Responsibilities

Senior Executive

(7) The Senior Executive are accountable for:

- ensuring data governance is aligned to the University's strategic objectives; and
- the final point of escalation in relation to data governance issues, including non-compliance of this Policy which will be handled under the [Code of Conduct](#).

Chief Data and Analytics Officer

(8) The Chief Data and Analytics Officer is responsible for:

- establishing and maintaining the University's Data Governance Framework;
- promoting good data governance by working with data custodians to ensure they embed data governance requirements across the data assets for which they are accountable; and
- ensuring appropriate processes are in place to enable data security on reports, dashboards, Application Programming Interfaces (APIs) and the University's data warehouse.

Data Modelers, Data Engineers and Business Analysts

(9) Data Modelers, Data Engineers and Business Analysts are responsible for:

- ensuring that data is accurately defined, modeled, stored, and transmitted in alignment with business, technical and legislative requirements;
- ensuring data assets conform to the University's Data Governance Framework;

- c. ensuring the relevant Data Custodian (or delegate) has approved the use of the data in advance;
- d. reporting data asset security risks or incidents to the Chief Information Security Officer (CISO); and
- e. reporting privacy risks or incidents in accordance with the [Privacy Policy](#).

Privacy Officer

(10) The Privacy Officer is responsible for:

- a. providing privacy advice as follows:
 - i. advice to Data Custodians and Data Stewards to help inform the data sensitivity; and
 - ii. advice on what legislation informs data classifications;
- b. providing privacy training to employees and raising awareness about the importance of privacy in data governance; and
- c. receiving and assessing privacy incidents and concerns.

Data Custodians

(11) Data Custodians are accountable for:

- a. the data assets associated with the operational units which they manage (e.g., the Chief People Officer (P&C) is responsible for staff-related data assets);
- b. accuracy of data assets, including definitions, data quality, and data classifications;
- c. setting and/or approving the conditions of use, including any system or storage requirements. They have the right to override the assigned security classification based on revised risk. However, care must be taken to ensure data is protected;
- d. ensuring access is on a 'need to know basis' and conforms with:
 - i. privacy law obligations; and
 - ii. security and data classification requirements; and
- e. complying with the University's record keeping requirements in relation to the storage, retention and destruction of data.

(12) All Data Custodians are members of the Data Governance Committee (which is outlined in more detail below).

Data Stewards

(13) Data Stewards are responsible for:

- a. managing day-to-day data-related activities as directed by the Data Custodian;
- b. assigning the data and security classifications for which they are responsible; and
- c. contributing to Data Governance Working Groups providing expertise on data assets associated with their operational unit.

Chief Information Officer (CIO)

(14) The Chief Information Officer (CIO) is responsible for:

- a. ensuring adequate security controls are in place to protect data against unauthorised access, breaches, and other security threats;
- b. prioritising data security in alignment with the nature of the risk; and
- c. ensuring data protection from unauthorised disclosure or interception.

(15) Overseeing the management of platforms (e.g. databases, file systems, communication channels).

Chief Information Security Officer (CISO)

(16) The Chief Information Security Officer (CISO) is responsible for:

- a. the technical management, security, and maintenance of data assets, in particular:
 - i. implementing and maintaining the IT infrastructure that supports data storage, processing, and transmission;
 - ii. ensuring data is securely backed up, reliably recovered, and protected from unauthorised access through robust security measures and access controls; and
- b. conducting regular audits and implementing updates and patches to maintain system security and efficiency.

Technical Custodians

(17) Technical Custodians (sometimes referred to as IT Administrators) are responsible for:

- a. working with data stewards, business analysts, and other stakeholders to enforce data governance;
- b. the technical aspects of data lifecycle management, including data archiving, purging, ensuring data integrity, and managing access controls; and
- c. additional information in the [Information Security Policy](#) under IT Administrators.

Records Management

(18) Records Management is responsible for:

- a. data retention, ensuring that data is retained in compliance with legal and regulatory requirements and supports data lifecycle management; and
- b. auditing and reviewing data retention and disposal practices to ensure compliance.

Part B - Data Governance Committee

(19) The Data Governance Committee is a forum for Data Custodians and other designated officials (who have planning, policy level and management responsibility for data within their functional areas) to discuss data assets.

(20) The Data Governance Committee will:

- a. meet regularly and upon the request of Chief Data and Analytics Officer;
- b. monitor data quality;
- c. promote data literacy, awareness, and appropriate data use; and
- d. ensure alignment with the strategic plan.

Part C - Data Classification

(21) Data classification is required to ensure that data is managed in a manner proportionate to its sensitivity, criticality, and strategic value. It enables custodians and stakeholders to make informed decisions regarding data access, sharing, storage, and disposal.

(22) All data assets must be classified in accordance with the Data Classification Policy. Classification must consider factors such as sensitivity, the presence of personal or confidential information, regulatory obligations, and business impact.

(23) Assigned classifications must be used to determine and enforce appropriate handling, protection, and access controls, in alignment with the [Information Security Policy](#) and relevant standards.

(24) Data custodians are accountable for ensuring that data is appropriately classified at creation or acquisition, reviewed periodically, and updated where required to reflect changes in use, risk, or value.

(25) Refer to the Data Classification Policy (drafted).

Part D - Information Security Classification

(26) Data is secured through the application of controls defined in the [Information Security Policy](#), aligned to its data classification, and regulatory obligations.

(27) Refer to the [Information Security Policy](#).

Part E - Reference Data

(28) Reference data must be defined, standardised, and governed to ensure the consistent use of codes, values, and hierarchies across the organisation. It provides a common foundation for data integration, reporting, data quality, analytics, and operational processes.

(29) Reference data must be managed in accordance with approved standards and governance processes, including defined ownership, version control, and controlled change management to maintain integrity and traceability over time.

(30) Data stewards are responsible for ensuring the accuracy, completeness, and ongoing relevance of reference data within their data domain, and for supporting its appropriate use across business and technology functions.

(31) The use of reference data must be enforced on any application implementations where possible, to promote consistency, reduce duplication, and enable interoperability across the enterprise.

(32) Reference data must be consistently applied in reporting, analytics, and integration processes to minimise transformation effort, reduce cost of change, and improve data literacy through the use of standardised and well-understood values.

Part F - Master Data

(33) Master data must be defined, governed, and managed as a critical enterprise asset to provide a single, consistent, and authoritative source of core business entities.

(34) All master data entities must have a business definition recorded in the enterprise data governance catalogue, with clear linkage to the relevant data domain, accountable stakeholders (including data custodian and stewards), and the identified system of record.

(35) Data custodians and stewards are accountable for ensuring the accuracy, completeness, consistency, and uniqueness of master data, including the resolution of duplicates and ongoing maintenance.

(36) Master data must be shared and reused across systems to enable integration, reduce duplication, and support consistent, reliable reporting, analytics, and operational processes.

(37) Master data must be subject to ongoing data quality monitoring, with defined rules, validation processes, and remediation workflows to maintain trust and reliability over time.

Part G - Data Quality

(38) Ensures data is trusted, accurate, consistent, and fit for purpose across operational and reporting environments.

(39) Industry-standard data quality dimensions are used, including accuracy, completeness, consistency, validity, timeliness, uniqueness, and integrity.

(40) We use the “shift-left” approach to data quality, where issues are resolved as close to the source system and point of data capture as possible. Responsibility for maintaining data quality sits with business stakeholders, data custodians, and system owners who create the data.

(41) Data Governance teams are not responsible for cleansing or correcting data. The Data Governance team create data quality rules to monitor and profile data, and provide visibility of data quality issues through reporting, scorecards, and dashboards to support remediation activities.

(42) Data quality issues identified through monitoring, profiling, or stakeholder feedback may be raised through the Data Governance Committee for prioritisation and remediation planning based on business impact, risk, and operational requirements. Remediation should focus on improving business processes and source systems to deliver sustainable long-term data quality improvements.

Part H - Data Domains and Subdomains

(43) Provide a structured framework to organise enterprise data assets, enabling clear custodianship, governance, and cataloguing.

(44) Each assigned a Data Custodian who is accountable for the oversight assignment of custodianship documented on the Data Governance Framework within Data Stewardship.

(45) The creation of top-level data domains should adhere to the following principles:

- a. Alignment with Business: Domains must directly reflect and support core business functions or areas of expertise; and
- b. Distinct Business Context: The domain must represent a significant area within the business with its own specific meaning and usage patterns.

(46) Subdomains are used to further refine and organise data within a domain. A subdomain should be created only when one or more of the following principles are met:

- a. Specialised Governance Needs: The data within the subdomain requires specific policies, access controls, or classification measures that differ from the parent domain;
- b. Independent Ownership: A specific team or person is primarily responsible for the data within the subdomain, and this ownership justifies a separate subdomain; and
- c. Unique Data Quality Requirements: The data within the subdomain has unique data quality needs or requires specific validation rules that are different from the parent domain.

Section 7 - Definitions

(47) For the purpose of this Policy and Procedures:

- a. Business Domain: an area of responsibility or a grouping of naturally coherent concepts.
- b. Business Entity: a business entity encapsulates data with common characteristics. It is used to align, Data

Governance, Data Flow Diagrams, Integration, Conceptual Models and Logical Models, Data Sources.

- c. Business Term: the definition of key business information that is used in day-to-day business operations and analysis. Business terms also help to provide the link from information to the underlying data.
- d. Data: any recorded information and can include technical data, financial information, management information, representation of facts, numbers or data of any nature that can be communicated, stored and processed.
- e. Data Asset: is a resource that is owned and controlled, is expected to be of value and to generate positive future economic benefit.
- f. Data attribute: this is the smallest unit of data, the column or field level in tables and files.
- g. Data classification: is the process of separating and organizing data into relevant groups ("classes") based on their shared characteristics, such as their level of sensitivity, the risks they present, and could be the compliance regulations that protects the data.
- h. Data governance framework: is a structured approach that ensures data assets are managed effectively, efficiently, securely, and in compliance with relevant regulations and policies. It encompasses the processes, roles, policies, standards, and technologies.
- i. Data set: the collection of data attributes within a business context. A data set may be in the format of a flat file, database table, report, application programming interface (API), etc.
- j. Data Entity Model: La Trobe's Data Entities originally derived from the Higher Education Data Reference Model published by the Council of Australasian University Directors of Information Technology (CAUDIT). It defines our core data concepts allowing categorisation for a reference point for data management.
- k. Health information: health information has the meaning set out in the [Health Records Act 2001 \(Vic\)](#). Health information is personal information: about the physical, mental or psychological health or disability of an individual; about an individual's expressed wishes regarding the future provision of health services to them; about a health service provided, or to be provided, to an individual; collected to provide a health service; about an individual collected in connection with organ or body substance donation; or that is genetic information in a form which is or could be predictive of the health of the individual or of their descendants.
- l. Personal information: has the meaning set out in the [Privacy and Data Protection Act 2014 \(Vic\)](#) and includes information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
- m. Sensitive information: personal information about an individual's racial or ethnic origin, political opinions, membership of a political, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices or criminal record.

Section 8 - Authority and Associated Information

(48) This Policy is made under the [La Trobe University Act 2009](#).

(49) Associated information includes:

- a. [Records Management Policy](#)
- b. [Information Security Policy](#)
- c. [Research Data Management Policy](#)
- d. [Code of Conduct](#)
- e. [Risk Management Policy](#)
- f. [Critical Incident and Business Continuity Management Policy](#)
- g. Data Governance Framework (under development)
- h. Data Classification Policy

Status and Details

Status	Current
Effective Date	30th October 2026
Review Date	8th October 2029
Approval Authority	Vice-Chancellor
Approval Date	30th October 2026
Expiry Date	Not Applicable
Responsible Manager - Policy	Nina Clemson Chief Data and Analytics Officer
Enquiries Contact	Data and Performance Analytics

Glossary Terms and Definitions

"student" - Student is defined in the La Trobe University Act 2009 as: (a) a person enrolled at the University in a course leading to a degree or other award; or (b) a person who is designated as a student or is of a class of persons designated as students by the Council.

"staff" - Staff means any person employed by the University as per the definition in the La Trobe University Act 2009 (Vic).

"CONAGOTH" - Consultants, Agency or Other