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	13 November 2027

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, human resources data, course data, and subject data.

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

Section 3 - Scope

(4) This Policy applies to:

a. all institutional data;
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.

Section 4 - Key Decisions

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

Key Decisions	Role
Implement security measures to safeguard sensitive data, both from external threats (such as cyberattacks) and internal risks (such as unauthorized access). This may involve setting up firewalls, encryption, access controls, and security protocols.	IS Custodians
Work with the different internal entities (information security, corporate risk, and compliance risk) to define the policies and programs to ensure data delivery, protection, and retirement.	Chief Data and Analytics Officer
Monitor and provide guidance on collection, legal and regulatory requirements to ensure compliance with data protection laws and advise on data sensitivity classifications for Personal Information (PI).	Privacy Officer
Approve data sources for metadata scanning and profiling.	Data Information Governance Council (DIGC)

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:

a. Institutional data is an asset of the University
b. It is governed through defined roles and responsibilities
c. Individuals are responsible for the data they collect and manage on behalf of the University
d. Data must be of good quality e.g. accuracy, completeness, consistency, timeliness, validity and uniqueness, and managed consistently across its lifecycle
e. The management of institutional data must comply with applicable legislation and relevant policies
f. 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 Chief Operating Officer is accountable for the University's Data Governance. They are:

a. responsible for ensuring it is adequately resourced and aligned to the University's strategic objectives; and
b. 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.

Data and Analytics & Associated Roles

Chief Data and Analytics Officer

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

a. establishing and maintaining the University's Data Governance Framework;
b. promoting good data governance by working with data owners to ensure they embed data governance requirements across the data assets for which they are accountable; and
c. 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:

a. ensuring that data is accurately defined, modeled, stored and transmitted in alignment with business, technical and legislative requirements;
b. ensuring data assets conform with the University's Data Governance Framework;
c. ensuring the relevant Data Owner 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 Owners and Data Stewards to help inform the data sensitivity
    ii. advice on what legislation inform data classifications
b. providing privacy training to employees and raising awareness about the importance of privacy in data governance
c. receiving and assessing privacy incidents and concerns.

Data Owners & Data Stewards

Data Owners (also sometimes referred to as Data Custodians)

(11) Data Owners are senior managers who are accountable for the data assets associated with the operational units which they manage (e.g. the Executive Director, Human Resources (HR) is responsible for HR-related data assets).

(12) A Data Owner is accountable for:

a. accuracy of data assets, including definitions, data sets, data and security classifications;
b. 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;
c. ensuring access is on a 'need to know basis' and conforms with:
    i. privacy law obligations; and
    ii. security and data classification requirements.
d. complying with the University's record keeping requirements in relation to the storage, retention and destruction of data.

(13) All Data Owners are members of Data Information Governance Council (which is outlined in more detail below).

Data Stewards

(14) Data Stewards are appointed by the Data Owner to support them in managing day-to-day data-related activities.

(15) A Data Steward is responsible for:

a. assigning the data and security classifications for which they are responsible
b. contributing to the Data Governance Working Group, the function of which is described in more detail below

c. providing expertise on data assets associated with their operational unit

Information Services

Chief Information Officer (CIO)

(16) The Chief Information Officer is accountable 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 regards to the nature of the risk;
c. ensuring data protection from unauthorised disclosure or interception;
d. overseeing the management of platforms (e.g. databases, files system, communication channels).

Chief Information Security Officer (CISO) & Information Services (IS) Custodian

(17) The CISO & IS Custodians are 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;
b. working with data stewards, business analysts, and other stakeholders to enforce data governance;
c. the technical aspects of data lifecycle management, including data archiving, purging, and ensuring data integrity;
d. conducting regular audits and implementing updates and patches to maintain system security and efficiency.

Information Architects

(18) The Information Architect is responsible for:

a. ensuring consistency and interoperability across system integrations;
b. data architecture for the organisation, including the enterprise data model, application register and their associated data business entities;
c. overseeing the data lifecycle, from creation to disposal, balancing business needs with regulatory requirements;
d. ensuring data quality to utilise the full potential of data assets while also mitigating risks associated with data governance.

Records Management

(19) The Records Management Office is responsible for:

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

Part B - Governance Structure

Data Information Governance Council (DIGC)

(20) The Data Information Governance Council is a forum for Data Owners and other designated officials (who have planning, policy-level, and management responsibility for data within their functional areas) to discuss data assets.

(21) The Data Information Governance Council 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
d. ensure alignment with the strategic plan

Data Governance Working Group (DGWG)

(22) The Data Governance Working Group consists of data governance leads, data stewards, subject matter experts, data modelers, Privacy Officer, Information Services security, digital records representatives and information architects.

(23) The Data Governance Working Group will:

a. monitor and review business terms, metrics, enterprise information model updates, data sets, data classifications, reference data, marketplace collections and data quality rules.

Part C - Classifications

(24) Data classifications are used to manage and protect data based on sensitivity, value, and regulatory requirements. Security classifications protect information e.g. documents, data sets, business terms and metrics. Both classifications ensure handling of data is compliant with laws, regulations, policies and standards throughout its lifecycle. To do this institutional data is to be classified as follows:

Sensitivity Classification

(25) The classification is based on the impact disclosing the data has on the University:

a. None – data that is not sensitive and poses no risk to the University if exposed or accessed by unauthorised individuals.
b. Low - data that has a low impact on the University if exposed or accessed by unauthorised individuals.
c. Medium - data that could pose a moderate risk to the University if exposed or accessed improperly.
d. High - data that has a significant impact on the University if accessed, or modified without authorisation.

(26) Data sensitivity classification can be used for data security, compliance, incident response and data lifecycle management.

Security Classification

(27) The classification determines the level of protection on the information:

a. Public – freely disclosed to the public without any risk of harm to the University. Is for open access and does not require special handling.
b. Internal - intended for use within the University and not for public disclosure. Unauthorised access could cause moderate harm but typically would not have severe consequences.
c. Confidential - if disclosed without authorisation, could cause significant harm. Access is usually limited to

specific individuals or groups.

d. Restricted - highest level of classification and is applied to information that, if disclosed without authorisation, could cause severe damage.

Section 7 - Definitions

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

a. Data Asset: is a resource that is owned and controlled, is expected to be of value and to generate positive future economic benefit.
b. Business Domain: an area of responsibility or a grouping of naturally coherent concepts.
c. 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.
d. 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.
e. Data: any recorded information and can include technical data, computer software documents, financial information, management information, representation of facts, numbers, or datum of any nature that can be communicated, stored, and processed.
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. Enterprise Information Model: La Trobe’s Enterprise Information Model is derived from the Higher Education Data Reference Model published by the Council of Australasian University Directors of Information Technology (CAUDIT). It defines our foundation, enabling and core business domains to allow further data categorizing into each domain’s business entities. It provides a reference point for all data management activities.
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. Security Classification: The process of categorizing information assets based on the level of protection required. This classification helps in determining the appropriate security controls, access restrictions, and protective measures required to safeguard the data from unauthorized access, disclosure, or misuse.
n. 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

(29) This Policy is made under the La Trobe University Act 2009.

(30) 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)

Status and Details

Status	Current
Effective Date	13th November 2024
Review Date	13th November 2027
Approval Authority	Vice-Chancellor
Approval Date	13th November 2024
Expiry Date	Not Applicable
Responsible Manager - Policy	Nina Clemson Chief Data and Analytics Officer
Author	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).