Data Governance Policy

Section 1 - Background and Purpose

(1) Data Governance is the overall process of managing data throughout its lifecycle.

(2) Data is any recorded information and can include technical data, representation of facts, numbers or datum of any nature that can be communicated, stored and processed.

(3) Institutional data is defined as data that is created, received, maintained and/or transmitted by the University in the course of its operations. Institutional data is used for reporting and decision making and includes enrolment data, financial data, human resources data, course and subject data.

(4) This Policy establishes the Data Governance Framework, and sets out the fundamentals, roles and responsibilities and requirements for effective institutional data management.

Section 2 - Scope

(5) This Policy applies to:

a. All institutional data used in the administration of the University.
b. Students, employees, contractors and other third parties who, in the course of their work or studies, have access to the University's information, information systems and other facilities on the computer network.

(6) This Policy excludes:

a. Research data as defined in Research Data Management Policy.

Section 3 - Policy Statement

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

a. Institutional data is a strategic asset of the University
b. It is governed through a defined role and responsibility structure
c. All staff are accountable for the data they collect and manage on behalf of the University
d. Data must be of good quality and managed consistently across its lifecycle to enable accurate reporting and support evidence-based decision making
e. The management of institutional data is compliant with applicable laws, regulation and standards
f. Institutional data is held securely and protected from unauthorised access, use and disclosure

(8) In order for Institutional data to be a strategic asset, it requires robust governance and management practices to ensure that the value of data is achieved and preserved for future benefits. A Data Governance Framework has been created to provide overarching management of institutional data with the purpose of establishing its value and

realising its benefits. The Data Governance Framework consists of the core elements of data custodianship, data management, data quality, and data analytics and institutional reporting.

Section 4 - Procedures

Part A - Data Custodianship and Roles

(9) Data Custodianship is the administrative and/or operational responsibility for institutional data.

(10) The area of custodianship is determined by the Business Domains outlined in the Enterprise Information Model.

(11) Data Custodianship is facilitated by two key roles:

a. Data Custodian: has the overall administrative and/or operational responsibility of the Business Domain's information i.e Human Resources, Finance, Student Administration; and
b. Data Steward: is appointed by the Data Custodian and supports the Data Custodian in managing the day-to-day activities involved in data custodianship.

(12) The purpose of Data Custodianship is to ensure that institutional data is compliant with applicable laws, regulation and standards, both internal and external.

(13) The Data Custodian a Business Domain is responsible for:

a. Enterprise Applications also referred to as 'Source Systems', that are used to conduct the day-to-day business activities within a Business Domain.
b. Shared Enterprise Data Stores are data repositories for storing and managing institutional data for the purpose of institutional reporting and supporting data analytics.

(14) Further detailed descriptions of responsibilities for each key role are available via the Data Governance Intranet.

(15) The Director of Data and Analytics, in consultation with the Chief Information Officer, is responsible for appointing positions to data governance roles under the Data Governance Framework.

(16) The Data Governance RACI matrix outlining key roles and responsibilities across the Data Governance program is available via the Data Governance Intranet.

Part B - Data Management

(17) All institutional data must:

a. be part of the Enterprise Business Capability Model;
b. be categorised into a Business Domain as outlined in the Enterprise Information Model;
c. adhere to the University's Enterprise Data Architecture, classification, storage and security protocols.

Data Architecture

(18) Architecture: Involves the process of designing, acquiring, modelling and integrating data and is further expanded in the Data Governance Intranet.

(19) The arrangements within data architecture incorporate the following:

a. Data Modelling:

    i. Enterprise Information Model
    ii. Data Context and Scoping
    iii. Conceptual Data Modelling
    iv. Logical Data Modelling
    v. Physical Data Modelling

b. Data Ingestion and Consumption Management including:
    i. Data Solution Review
    ii. Data Conflicts Mediation
    iii. Data Service Design
    iv. Data Migration Design
    v. Data Requirements and Mapping
    vi. Data Linkage Management
    vii. Data Lineage Management

c. Data Auditing

(20) Detailed descriptions of the data architecture procedures are contained within the Data Governance Intranet.

Data Classification

(21) Institutional Data is to be classified in accordance with the Data Classification Scheme and be assigned with one of four classification levels:

a. protected
b. in-confidence/confidential
c. internal only (default)
d. public

(22) Data that has not been classified into one of the four categories, shall default to the internal only classification level.

(23) If data can fall into more than one classification level, the more restrictive classification level must be used.

(24) The Data Custodian is responsible for assigning the classification level to data within their Business Domain and must consider the:

a. sensitivity and/or value of the asset and level of protection to be applied;
b. confidentiality, integrity and availability of the asset, as described in the Information Security Policy;
c. intended distribution relative to the confidentiality, integrity and availability profile of the asset;
d. balance the day to day needs of operations management with the intended outcomes; and
e. changes can occur after the initial data classification and can be initiated through periodic review or when additional data or information becomes available.

(25) Before Institutional data is classified as Protected or In-Confidence, or any data that is changed from these classification levels, consultation is required with:

a. Legal Services
b. the Privacy Officer
c. the Data Governance Manager

d. IS Security
e. Assurance Group
f. other appropriate senior staff members or committees, as appropriate for the data asset.

(26) Where a conflict exists between contractual, legal or regulatory requirements, the more restrictive classification level should be applied.

Data Security

(27) All institutional data must be held securely and protected from unauthorised access, use and disclosure.

(28) Access to Shared Enterprise Data stores is restricted, controlled and managed in accordance with the Information Security Policy.

(29) Data Stewards are responsible for approving new or changed user access based on the specific role of a user. Aligning with the Information Security Policy, a formal registration process must be in place for granting, changing or revoking access to data (refer to Part A – Data Custodianship). Data Stewards, in conjunction with the Information Services Security team are to periodically audit user access.

(30) Data that is ingested into Shared Enterprise Data stores for the purposes of reporting and analysis must:

a. adhere to the principles outlined in the University's Privacy Policy
b. be located on storage media with appropriate security and protection protocols and be as secure as its source system
c. reflect the data classification level that was assigned by the Data Custodian in the Enterprise Application

(31) Data Custodians must ensure that data is suitable for consumption, made available for reporting and analysis and can be used in combination with other data.

(32) New data that is derived in Share Enterprise Data stores must consider the originating data source and will be classified in consultation with the Data Custodian where appropriate.

(33) Users are responsible for ensuring the protection of data in Shared Enterprise Data stores and must ensure good data security practices including:

a. protecting dashboards, reports or raw data from unauthorised access, irrespective of the device or location;
b. generating reports and outputs that comply with privacy principles;
c. only distributing reports, analysis and data to authorised recipients;
d. maintaining the data classification and protection levels in reports and outputs generated throughout the data lifecycle; and
e. reporting any detected or suspected data security events or weaknesses to the relevant Data Steward.

(34) Data Custodians and/or Data Stewards are responsible for ensuring data classification levels are maintained and periodically auditing compliance with the data classification levels used in reports and analytics.

Data Security Events or Weaknesses

(35) Users of information systems or services must report any detected or suspected security events or weaknesses to the relevant Data Steward as soon as possible.

(36) Where a data security event (actual, potential or suspected) involves personal information, the user and/or Data Steward must notify the University's Privacy Officer on (03) 9479 1839 or privacy@latrobe.edu.au as soon as possible,

or in any event 24 hours of discovery as per the University's Data Breach Response Plan.

(37) Major data security events and/or breaches will be managed in accordance with the University's Critical Incident and Business Continuity Management Policy.

Data Storage

(38) Institutional data must be stored on appropriate storage media as outlined in the Data Storage Classification Matrix.

(39) A data storage environment must ensure that:

a. Digital institutional data is backed-up at appropriate and scheduled intervals
b. Appropriate authentication and authorisation is implemented
c. Threat management software, that is supported by Information Services is applied
d. The secure transfer of data is maintained
e. Appropriate data sovereignty is maintained
f. Data is stored in accordance with the Records Management Policy

(40) The Data Custodian is responsible for defining the 'useful life' of data within their Business Domain which will be driven by business practice and usefulness. The 'useful life' of data may differ between Enterprise Applications and Shared Enterprise Data stores.

(41) The 'useful life' may be different to the retention period prescribed by the Public Records Act 1973; therefore the 'useful life' will not override the prescribed minimum retention period.

(42) The retention, archiving, disposal or transfer of institutional data must be performed in accordance with the Records Management Policy and in consultation with the Data Custodian.

Part C - Data Quality

(43) Data Quality is defined as the fitness of data to serve its purpose in a given context.

(44) The University uses a Data Quality Assessment Framework to measure and monitor Data Quality.

(45) Data Quality includes Institutional data being compliant with applicable laws, regulation and standards, both internal and external.

(46) The Data Custodian is responsible for the overall quality of data within their Business Domain.

(47) Users are responsible for notifying any data quality issues identified within Enterprise Applications or Shared Enterprise Data Stores through to Data Stewards.

(48) The Data Governance team, in partnership with Data Custodians and Data Stewards, is responsible for coordinating remediation activities to improve overall data quality.

(49) An extensive Business Glossary of business terms with clear definitions, meanings and business context is available via the Data Governance Intranet. The Business Glossary forms an integral part of Data Quality and is to be the source of truth for business terms, ensuring a common business vocabulary that is centred around the one definition.

(50) New terms and modifications to existing terms in the Business Glossary must be raised by Data Stewards, endorsed by Data Custodians and approved by the Data Governance Manager.

Part D - Data Analytics & Institutional Reporting

(51) Data Analytics is defined as the ability to analyse raw data from Shared Enterprise Data Stores in order to project future trends, scenarios, events and behaviours by developing machine learning algorithms and advanced analytical data models.

(52) Institutional Reporting is defined as the process of analysing current and historical data from Shared Enterprise Data Stores to present actionable insights on business performance, as a periodic Institutional Report or an interactive Dashboard, for strategic and operational decision making.

(53) All data analytics and institutional reporting required for the planning and the administration of the University must be aligned with Enterprise Data Architecture.

(54) The Data and Analytics team, in partnership with Data Custodians, Data Stewards and Information Services is responsible for facilitating:

a. the development and delivery of Data Analytics and Institutional Reporting;
b. the development and implementing of corporate model, frameworks and guidelines in relation to the management of data; and
c. overall management and coordination of the Data Analytics and Institutional Reporting portfolio across the University.

(55) Within their domain, the Data Custodian is responsible for ensuring Data Analytics and Institutional Reporting comply with this and all related procedures and guidelines.

Section 5 - Definitions

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

a. 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: describes an area of responsibility/business unit within the University and includes Human Resources, Finance, Student Administration etc.
c. Data Governance: the overall process of managing data throughout its lifecycle.
d. 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.
e. Data Management: an administrative task that includes acquiring, modelling, classifying, integrating, validating, processing, storing and securing institutional data.
f. Data Quality: An assessment of data’s fitness to serve its purpose in a given context. Key Data Quality components are Accuracy, Completeness, Reliability, Relevance Timeliness, Consistency.
g. Enterprise Applications – Information Technology Applications that are commissioned to conduct and support business activities i.e SISOne, SAP, Success Factors.
h. Institutional data: data that is created, received, maintained and/or transmitted by the University in the course of its operations, that is used for reporting and decision making and includes enrolment data, financial data, human resources data, course and subject data.
i. Shared Enterprise Data Stores: Integrated Data Repositories that are commissioned to provide easy access to quality data for reporting and analytics.

Section 6 - Related Documents

(57) The following are related documents:

a. Records Management Policy
b. Information Security Policy
c. Research Data Management Policy
d. Privacy Policy
e. Code of Conduct
f. Risk Management Policy
g. Critical Incident and Business Continuity Management Policy
h. Data Governance Intranet
i. Business Glossary
j. Enterprise Data Architecture

Status and Details

Status	Current
Effective Date	20th July 2021
Review Date	20th July 2024
Approval Authority	Vice-Chancellor
Approval Date	8th July 2021
Expiry Date	Not Applicable
Responsible Manager - Policy	Nina Clemson Chief Data and Analytics Officer
Author	David Noden
Enquiries Contact	Data and Performance Analytics