UNSW College

Data Governance Policy

1. Purpose

Corporate data is a strategic asset of UNSW College (the College). The appropriate governance for management and use of this data enhances the quality, availability, integrity and protection of the College's business operations and critical decision making. Lack of governance can lead to operational inefficiencies and could expose the College to unwanted risks.

The purpose of this Policy is to:

(a) define the roles and responsibilities for different data creation and usage types, cases and/or situations, and to establish clear lines of accountability;

(b) develop best practices for effective data management and protection;

(c) protect the College's data against internal and external threats (e.g. breach of privacy and confidentiality or security breach);

(d) ensure that the College complies with applicable laws, regulations, exchange and standards;

(e) ensure that a data trail is effectively documented within the processes associated with accessing, retrieving, exchanging, reporting, managing and storing of data.

2. Scope

This Policy applies to all College data used in its business operations, including academic and educational data. This Policy covers, but is not limited to, corporate data in any form, including print, electronic, audio-visual, backup and archived data.

This Policy applies to all employees, agents, secondees, contractors and interns.

3. Policy statement

3.1. Policy framework and principles

The Data Governance Framework (Appendix 1) outlines the principles and minimum standards that guide the College's governance procedures and must be adhered to by all College employees and other data users.

The Data Governance Framework aligns with the UNSW Data Governance Framework.

3.2. Governance and ownership

Role	Responsibility (Appendix 4)
Data Custodian	The College, rather than any individual business unit, is the Custodian of the data and any information derived from the data.
Data Executive	A Data Executive means an Executive.

	A Data Executive supported by a Data Owner has responsibility for the management of data assigned within their business unit.
Data Owner	Data Owners are delegated by a Data Executive, and are responsible for ensuring effective local protocols are in place to guide the appropriate use of their data asset. Access to, and use of, Corporate Data will generally be administered by the appropriate Data Owner. Data Owners (or a delegated Data Steward) are also responsible for ensuring that all legal, regulatory and policy requirements are met in relation to the specific data or information asset. This includes responsibility for the classification of data in accordance with the Data Classification Standard. Data Owners are responsible for ensuring that data conforms to legal, regulatory, exchange and operational standards. The Data Owner must ensure that the process for the administration of data is in accordance with the Data Management Life Cycle (Appendix 2).
Data Specialists	Data Specialists are business and technical Subject Matter Experts (SMEs) in relation to the data or information asset. The SMEs under the Management and Operations category (Appendix 3) are Information Technology specialists who will be responsible for providing ongoing support to College operational systems, data or informational assets.
Data Stewards	Some Data Areas have a Data Steward, who is responsible for the quality and integrity, implementation and enforcement of data management within their assigned area of responsibility. The Data Steward will classify and approve access, under delegation from a Data Owner, based upon the appropriateness of the User's role and the intended use. Where necessary, approval from the Data Executive/Data Owner may be required prior to authorisation of access.

3.3. Policy framework and principles

(a) Data users must ensure appropriate procedures are followed to uphold the quality and integrity of the data they access.

(b) Data records must be kept up-to-date throughout every stage of the business workflow and in an auditable and traceable manner.

(c) Data should only be collected for legitimate uses and to add value to the College. Extraction, manipulation and reporting of data must be done only to perform the College's business operation.

(d) Where appropriate, before any data (other than publicly available data) is used or shared outside the College, verification with the Data Owner or Data Steward is required to ensure the quality, integrity and security of data will not be compromised, and compliance obligations are maintained.

(e) Data shall be retained and disposed of in an appropriate manner in accordance with UNSW's Recordkeeping Policy, Recordkeeping Standard and associated procedures under the Privacy Act 1988 (Cth) and State Records Act 1988 (NSW).

3.4. Data classification and security

(a) College employees and other data users should refer to the Data Classification Standard and Data Handling Guidelines for further information.

(b) Appropriate data security measures (see the Data Classification Standard) must be adhered to at all times to assure the safety, quality and integrity of College corporate data.

(c) Personal use of corporate data, including derived data, in any format and at any location, is prohibited.

(d) Records stored in an electronic format must be protected by appropriate electronic safeguards and/or physical access controls that restrict access only to authorised user(s). Similarly, data in the College data repository (databases etc.) must also be stored in a manner that will restrict access only to authorised user(s).

(e) This Policy applies to records in all formats (paper, digital or audio-visual) whether registered files, working papers, electronic documents, emails, online transactions, data held in databases or on tape or disks, maps, plans, photographs, sound and video recording, or microforms.

3.5. Data terms and definitions

Terms used to describe different types of data should be defined consistently.

4. Roles, responsibilities and delegations

Role	Responsibility
Head of Information Technology	Implementing, disseminating and reviewing this Policy.
Business Intelligence Technical Manager	The day to day implementation of this Policy and being the first point of contact for enquiries.

5. Definitions

Definitions and Acronyms	
Access	The right to read, copy or query data.
Business Unit	Any organisational unit of the College. Without limiting any business units or divisions that may be formed from time to time, these include the following Business Units: (a) Education; (b) Finance; (c) Human Resources;

	(d) Information Technology; (e) Legal & Compliance; and (f) Sales & Marketing.
Corporate Data	A general term used to refer to the College's Data, including administrative and learning and teaching data.
Data	The representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means. Typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not Information until it is used in a particular context for a particular purpose. Data is typically considered to be conceptually at the lowest level of abstraction.
Data Area	A term used to denote a subset of Corporate Data that is the responsibility of a team including the Data Owner and Data Stewards (see section 4 for further details regarding these roles). This could include an entire IT system (e.g. SMS) or a Business Unit.
Data Governance	A quality control discipline for managing, using, improving and protecting organisational information.
Data Management Life Cycle	The process for planning, creating, managing, storing, implementing, protecting, improving and disposing of all the College's Corporate Data.
Data User (User)	Any Employee, agent, secondee, contractor or Intern who accesses, inputs, amends, deletes, extracts and analyses data in the College IT system to carry out their day-to-day duties. Data Users are not generally involved in the governance process, but are responsible for the quality assurance of data. Appropriate security and approval is required from the Data Owner to maintain the quality and integrity of the data. Data User also means any member of the College community who has access to Corporate Data, and thus is entrusted with the protection of that data.
Employee	A person who carries out work in any capacity for the College, including as an employee, contractor or subcontractor, employee of a contractor or subcontractor, employee of a labour hire company, outsourced employee, apprentice or trainee, Intern or volunteer.
Executive	The principal executive heading a business group or service function within the College (usually with the title Group Executive or Head of) who is a direct report to the Chief Executive Officer.
Integrity or Data Integrity	The accuracy and consistency of data over its entire life cycle.
Intern	A student or trainee who works temporarily for the College, sometimes without pay, in order to gain work experience or to satisfy requirements for a qualification.

Related Policy Documents and Supporting Documents	
Legislation	• Privacy Act 1988 (Cth) • State Records Act 1988 (NSW)
Policy	• UNSW Recordkeeping Policy • Information Security Policy
Procedures	• Data Classification Standard • Data Handling Guidelines • Data Breach Response Procedure • UNSW Recordkeeping Standard

6. Policy Governance

Data Governance Policy	
Category/Business Group	Legal and Compliance
Published Externally (Yes/No)	Yes
Approver	Chief Executive Officer
Responsible Officer	Chief of Staff
Contact Officer	Head of Information Technology
Effective Date	17/08/2023
Next Review Date	17/08/2026
Version	1.0

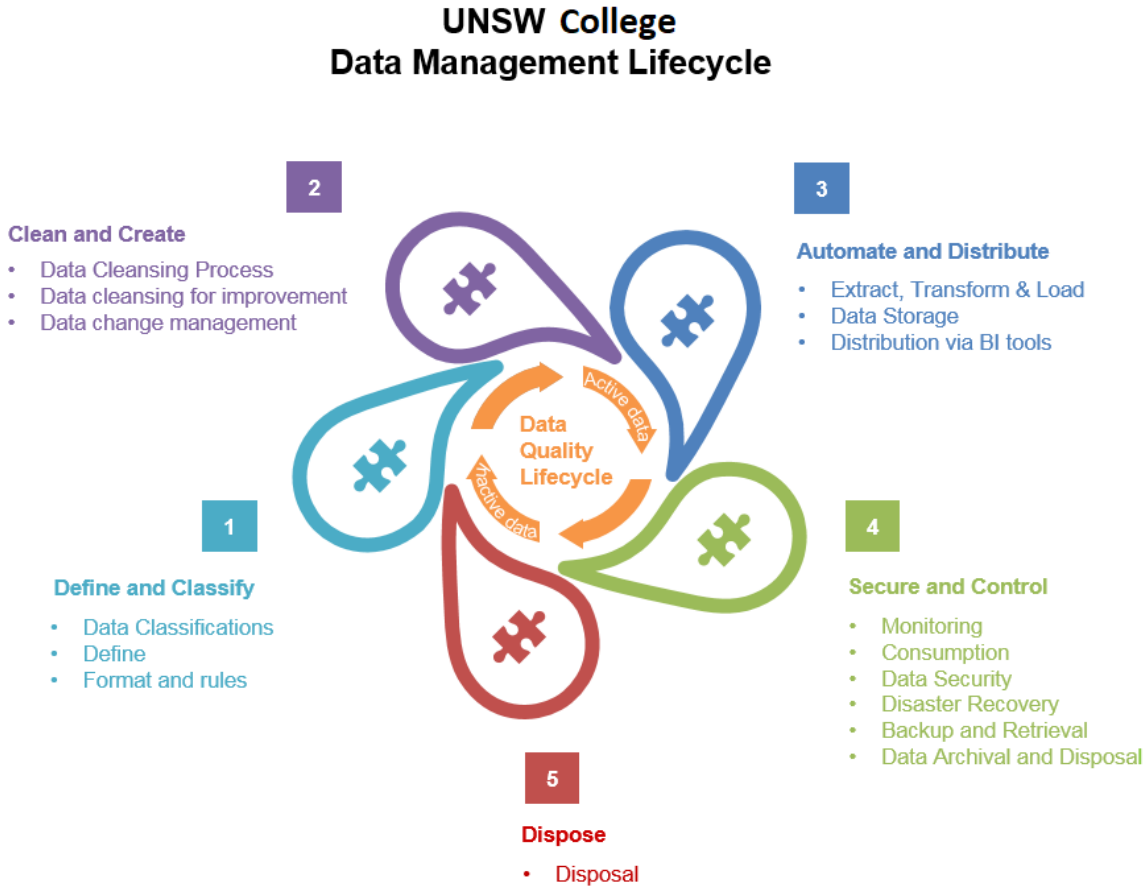
Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1	Chief Executive Officer – Sarah Lightfoot	11 August 2023	17 August 2023	N/A

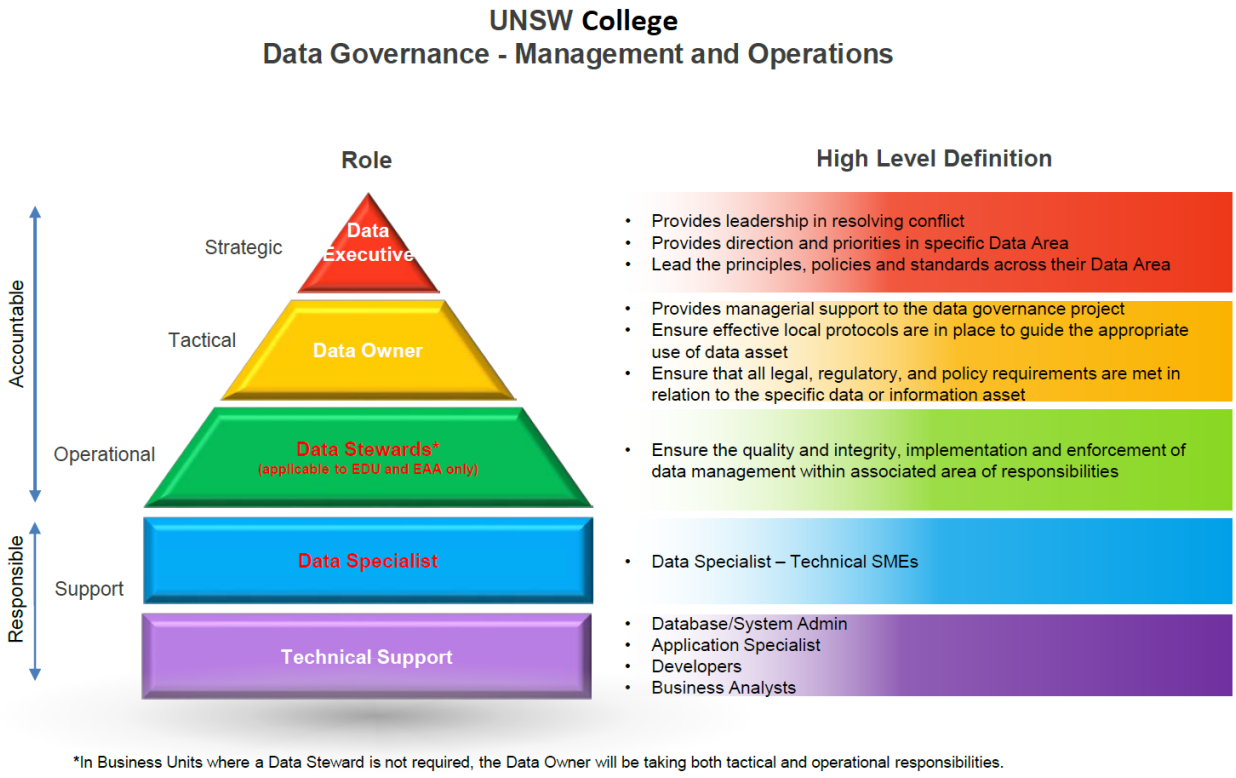
Please visit our website to ensure that you have the latest version of this Policy. Policies are available at: unswcollege.edu.au/about/policies

Appendix 1: Data Governance Framework

Appendix 2: Data Management Lifecycle

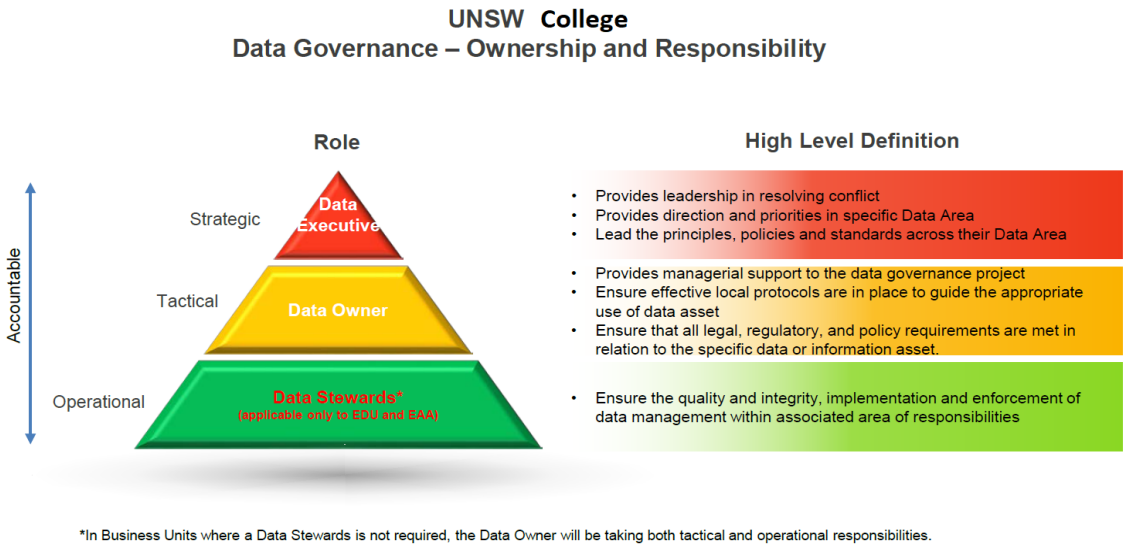


Appendix 3: Data Governance – Management and Operations



*In Business Units where a Data Steward is not required, the Data Owner will be taking both tactical and operational responsibilities.

Appendix 4: Data Governance – Ownership and Responsibility



*In Business Units where a Data Stewards is not required, the Data Owner will be taking both tactical and operational responsibilities.