POLICY	**DATA GOVERNANCE POLICY**
Area covered	This policy is University-wide

Version	**1.0**	**Approval date**	11 March 2016	**Effective date**	1 March 2016	**Next review date**	March 2019

Policy Statement

Purpose	Data policies are a collection of principles that describes the rules to control the integrity, security, quality, and usage of data during its lifecycle. The policy also defines the roles and responsibilities of University staff with internal and external parties in relation to data access, retrieval, storage, disposal, and backup of University data assets.
Scope	This policy applies to all UNSW staff

Policy Provisions

1. Background Information

Institutional data is a strategic asset of UNSW Australia (UNSW) and the appropriate governance for management and use of data is critical to the University's operations. Lack of governance can lead to operational inefficiencies and could expose the University to unwanted risks.

The Data Governance Framework (DGF) was introduced in the Data Governance Steering Committee meeting earlier 2015 to improve the oversight, guidance and quality of data. The framework focussed across People, Process, Technology and Governance to improve the management of data assets from a strategic and operational perspective. It allows UNSW to better leverage their data quality activities, business processes and capabilities. The framework was approved and endorsed by the committee for implementation. Data governance policies are a sub component of DGF. The policies are guided by principles that should be adhered to support the improvement in managing and securing the data across the University.

2. Policy Purpose

The purpose of the Data Governance Policy is to:

- Define the roles and responsibilities for different data usage and establish clear lines of accountability
- Develop best practices for effective data management and protection
- Protect the University's data against internal and external threats (e.g. breach of privacy and confidentiality)
- Ensure that the University complies with applicable laws, regulations, exchange and standards
- Ensure that a data trail is effectively documented within the processes associated with accessing, retrieving, exchanging, reporting, managing and storing of data

3. Policy Scope

This policy applies to all institutional data used in the administration of the University and all of its Organisational Units. This policy covers, but is not limited to, institutional data in any form, including print, electronic, audio visual, backup and archived data.

4. Policy Framework and Principles

The following framework outlines the principles and minimum standards that guide the University's data governance procedures and must be adhered by all UNSW staff:

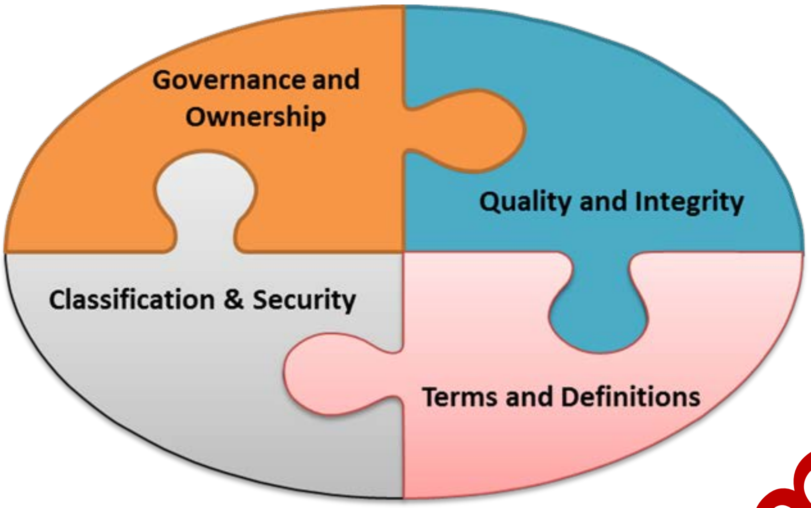
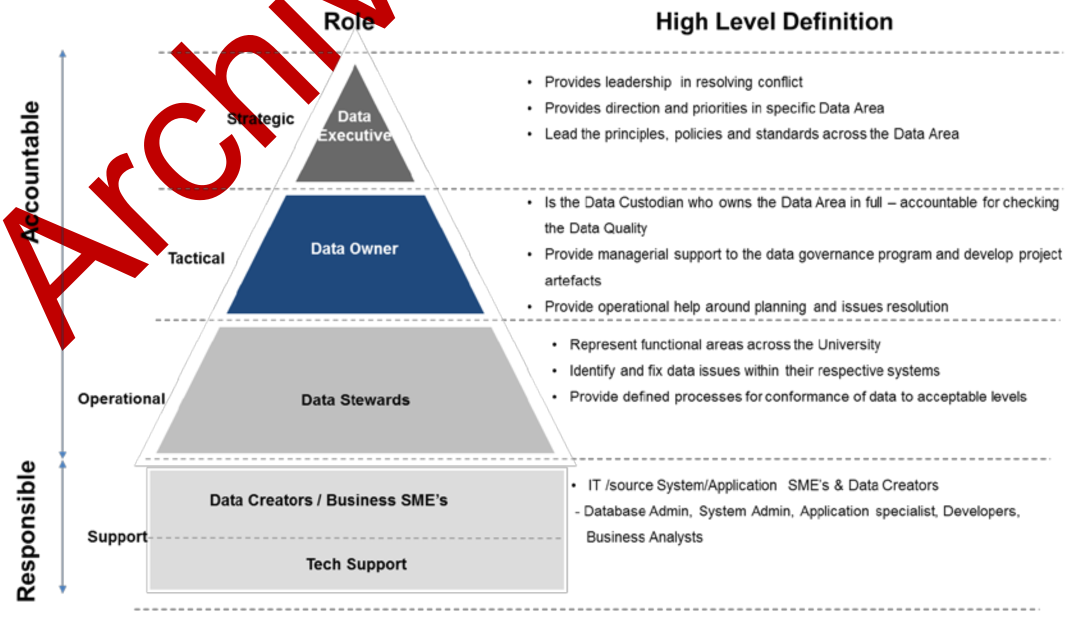


Figure 1.0: Data Policy Framework

A. Governance and Ownership

- UNSW, rather than any individual or Organisational Unit, is the owner of their data.
- Data Governance Steering Committee is responsible for the overall management of the University's Data Governance
- A Data Executive supported by a Data Owner has the responsibility for the management of data assigned within their portfolio
- Data Owners are Custodians, who are responsible for ensuring effective local protocols are in place to guide the appropriate use of their data asset. Access to, and use of, institutional data will generally be administered by the appropriate Data Owner
- Data Owner must ensure the process for the administration of data is in accordance with the Data Management Life Cycle (refer Appendix 1)
- Every data source must have a Data Steward, who is responsible for the quality and integrity, implementation and enforcement of data management within their Division



- Provides leadership in resolving conflict
- Provides direction and priorities in specific Data Area
- Lead the principles, policies and standards across the Data Area

- Is the Data Custodian who owns the Data Area in full – accountable for checking the Data Quality
- Provide managerial support to the data governance program and develop project artefacts
- Provide operational help around planning and issues resolution

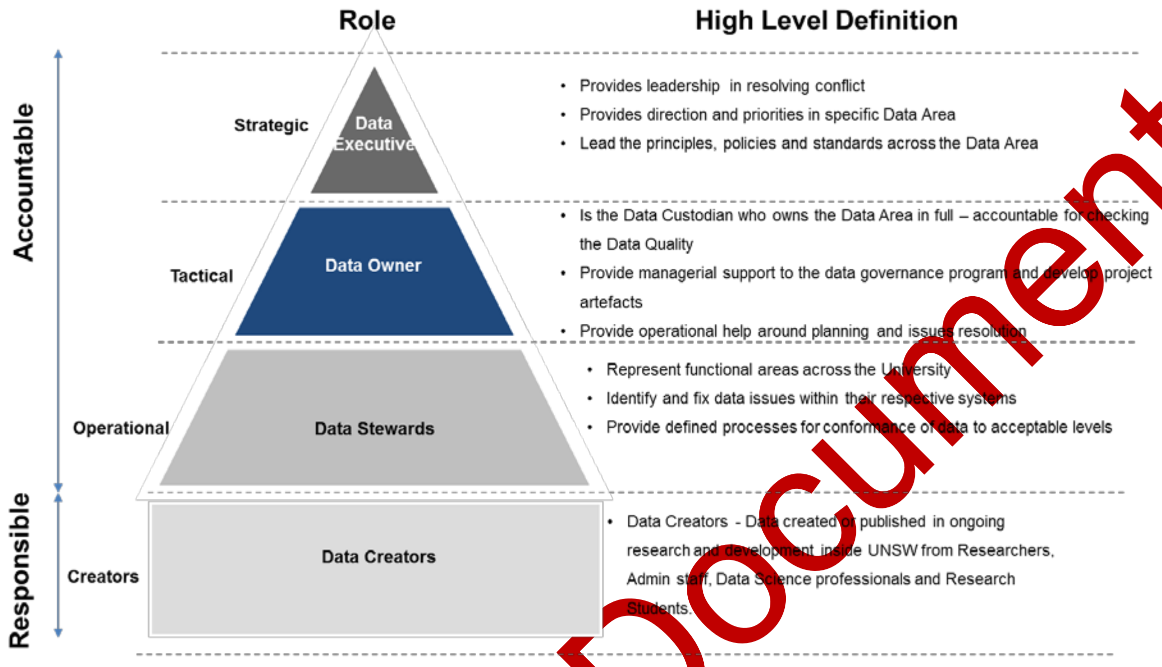
- Represent functional areas across the University
- Identify and fix data issues within their respective systems
- Provide defined processes for conformance of data to acceptable levels

- IT /source System/Application SME's & Data Creators

- Database Admin, System Admin, Application specialist, Developers, Business Analysts

Figure 2.0 – Data Governance Roles and Responsibilities – Management and Operations

- The Data Steward will classify and approve the access 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
- Data Creators or Business Subject Matter Experts (SME's) under **Management and Operations category** (refer fig 2.0) are Business or Information Technology specialists who will be responsible for providing ongoing support to UNSW Operational systems or data



- Provides leadership in resolving conflict
- Provides direction and priorities in specific Data Area
- Lead the principles, policies and standards across the Data Area

- Is the Data Custodian who owns the Data Area in full – accountable for checking the Data Quality
- Provide managerial support to the data governance program and develop project artefacts
- Provide operational help around planning and issues resolution

- Represent functional areas across the University
- Identify and fix data issues within their respective systems
- Provide defined processes for conformance of data to acceptable levels

- Data Creators - Data created or published in ongoing research and development inside UNSW from Researchers, Admin staff, Data Science professionals and Research Students.

Figure 3.0 – Data Governance Roles and Responsibilities – Ownership and Responsibility

- Data Creators under Ownership and Responsibility category (refer fig 3.0) are People who are responsible for the Creation and Ownership of research data and primary materials. Original research data and primary materials generated in the conduct of research at the University is owned and retained by the University, subject to any contractual, statutory, ethical, or funding body requirements. Researchers are permitted to retain a copy of the research data and primary materials for future use, subject to any contractual, statutory, ethical or funding body requirements.

B. Quality and Integrity:

- Data Creators and Data Users must ensure appropriate procedures are followed to uphold the quality and integrity of the data they access
- Data records must be kept up-to-date throughout every stage of the business workflow (University operations) and in an auditable and traceable manner. Data should only be collected for legitimate uses and to add value to the University. Extraction, manipulation and reporting of data must be done only to perform University business
- Where appropriate, before any data (other than publically available data) is used or shared outside the University, verification with the Data Steward is required to ensure the quality, integrity and security of data will not be compromised
- Data shall be retained and disposed of in an appropriate manner in accordance with the University's Records Keeping and associated procedures under NSW State Records Act 1988

C. Classification and Security:

- Personnel should refer to the Data Classification Standard and the Data Handling Guideline for further information.
- Appropriate data security measures (see Data Classification Standard document) must be adhered to at all times to assure the safety, quality and integrity of University data

- Personal use of institutional data, including derived data, in any format and at any location, is prohibited
- 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 University Data repository (Databases etc.) must also be stored in a manner that will restrict access only to authorised user(s)
- The 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 recordings, or microforms

D. Terms and Definitions

- The definition and terms used to describe different types of data should be defined consistently or referred to relevant Business Glossary of the University

5. POLICY REVIEW

This Policy will be reviewed and updated every five (5) years from the approval date, or more frequently if appropriate. In this regard, any staff members who wish to make any comments about the Policy may forward their suggestions to the Responsible Officer.

6. FURTHER ASSISTANCE

Any staff member who requires assistance in understanding this Policy should first consult their nominated supervisor who is responsible for the implementation and operation of these arrangements in their work area. Should further assistance be needed, the staff member should contact the Responsible Officer for clarification

APPENDIX 1 - DATA MANAGEMENT LIFE CYCLE

Data Management Life Cycle refers to the process for planning, creating, managing, storing, implementing, protecting, improving and disposing of all institutional data of UNSW.

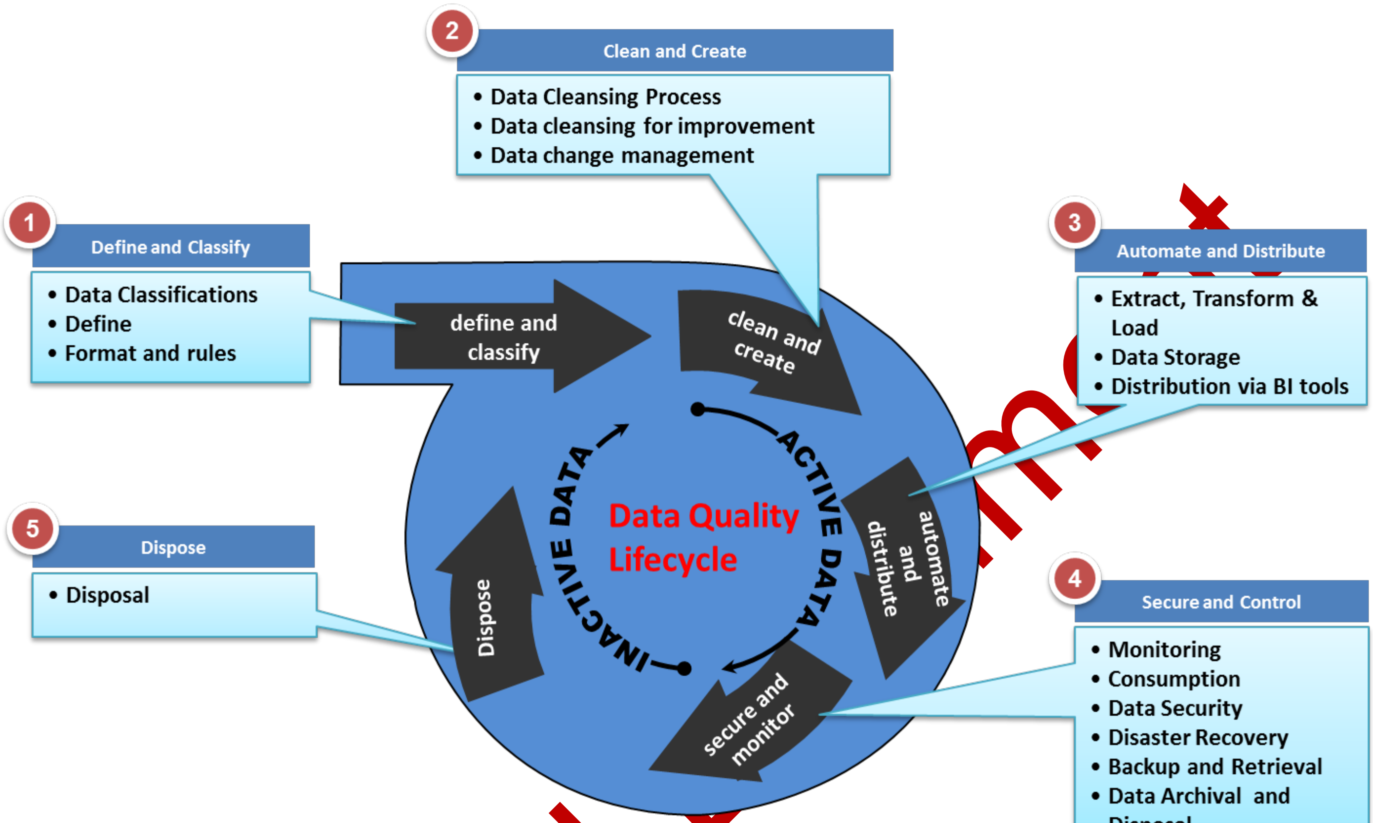


Figure 4.0 – Data Management Lifecycle

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	President & Vice-Chancellor	11 March 2016	1 March 2016	New Policy

Supporting Information

Supporting Documents	Data Classification Standard Data Handling Guideline
Related Documents	Nil
Superseded Documents	This is a new Policy
File Number	2016/09756
UNSW Statute and / or Regulation *Any variation to Policy or Procedure must remain consistent with the parent statute or regulation*	Nil UNSW Delegations of Authority https://www.gs.unsw.edu.au/registerofdelegations/index.html
Relevant State / Federal Legislation	Nil

Accountabilities

Responsible Officer	Director, Business Reporting & Intelligence, & Data Governance
Contact Officer	Deputy Director, Business Reporting & Intelligence, & Data Governance

Further Information

Key words for search engine	Data Governance, Data

Definitions and Acronyms

To establish operational definitions and facilitate ease of reference, the following terms are defined:

TERM	SYNONYMS	DEFINITION
Access		the right to read, copy, or query data
Data	Institutional Data	a general term used to refer to University's Data, both structured and unstructured stored in a Data repository, such as Database, which can generally be assigned to one of four categories: • **Public access data** – data that is openly available to all staff, students, and the general public. • **Internal general data** –

		data used for University administration activities and not for external distribution unless otherwise authorised. • **Internal protected data** – data that is only available to staff with the required access in order to perform their assigned duties. • **Internal restricted data** – data that is of a sensitive or confidential nature and is restricted from general distribution. Special authorisation must be approved before access or limited access is granted.
Record	Institutional Record	Metadata records stored in any digital format
Data Governance roles and responsibilities		outlines the access rights, roles and responsibilities of UNSW staff in relation to the management and protection of data
Data Governance Steering Committee	DGSC	Is a University wide committee, with members consisting of Data Executives, Data Stewards and designated Data Users. DGSC is responsible for approving the procedures related to the Data Governance Policy. DGSC also assures appropriate data processes are used in all of the University's data-driven decisions
Data Executive		Is a Senior Executive with planning and decision-making authority for UNSW's institutional data. The Data Executives, as a group, are responsible for overseeing the continuous improvement of the University's data governance and management
Data Steward		Is a Member of the Executive who oversees the capture, maintenance and dissemination of data for a particular Organisational Unit. Data Stewards are responsible for assuring the requirements of the Data Governance Policy and the Data Governance Procedures are followed within their Organisational Unit

Data Owner or Custodian		Has operational responsibilities in assisting Data Stewards with day-to-day data administration activities; including, but is not limited to: develop, maintain, distribute, and secure institutional data. Data Owners are expected to have high-level knowledge and expertise in the content of data within their responsible area. This role is also the organizational Data Custodian.
Data User		Any member of the university community that has access to university data, and thus is entrusted with the protection of that data.
Business SME		Is any staff member or authorised agent who accesses, inputs, amends, deletes, extracts, and analyses data in UNSW 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 Data Stewards to maintain the quality and integrity of the Data.
Data Creator		Data Creators who will be responsible for the Ownership of research data and primary materials. Original research data and primary materials generated in the conduct of research at the University will be owned and retained by the University, subject to any contractual, statutory, ethical, or funding body requirements. Researchers are permitted to retain a copy of the research data and primary materials for future use, subject to any contractual, statutory, ethical or funding body requirements.
Data Management Life Cycle		Refers to the process for planning, creating, managing, storing, implementing, protecting, improving and disposing of all institutional data of the University
Integrity or data integrity		Refers to the accuracy and consistency of data over its entire life- cycle
Data Quality	Quality	Refers to the validity, relevancy and currency of data

Security		refers to the safety of University data in relation to the following criteria: • Access control; • Authentication; • Effective incident detection, reporting and solution; • Physical and virtual security; and • Change management and version control.
Executive Team	ET	Is the peak senior strategic forum for UNSW, the ET is chaired by the Vice-Chancellor with members consisting of the Senior Deputy Vice-Chancellor, Deputy Vice-Chancellor Education; Chief of Staff / Deputy Vice-Chancellor; Deputy Vice- Chancellor Research; Deans.
Business/Division Area	Data Area	University Divisions, such as Finance, HR, Library, Students, etc.
SMS	Information Security Management System	In response to UNSW Data Classification and Handling requirements, the ISMS provides Information Security governance and sets out people, process and technology related controls to assure the confidentiality, integrity and availability of UNSW data. Moreover, the deployment and measurement of ISMS controls provides input into the risk management process enabling informed business decisions.