UNIVERSITY
OF WOLLONGONG
AUSTRALIA

DATA GOVERNANCE PROCEDURE

Date first approved:	Date of effect:	Date last amended: (refer to Version Control Table)	Date of Next Review:
9 February 2021	9 February 2021	9 February 2021	9 February 2022

First Approved by:	Chief Operating Officer
Custodian title & e-mail address:	Senior Manager, Information Management Unit – IMTS data-governance@uow.edu.au
Author:	Data Governance Coordinator, Information Management Unit
Responsible Division & Unit:	Information Management & Technology Services – Information Management Unit
Supporting documents, procedures & forms:	Cyber Security Policy Data Breach Response Plan Data Handling Guidelines Data Quality Management Procedure IT Acceptable Use Policy IT Server Security Policy IT User Account Management Procedure Learning Analytics Data Use Policy Privacy Impact Assessment Tool Privacy Policy Records Management Policy Research Data Management Policy Research Data Management Guidelines University Code of Conduct
Relevant Legislation & External Documents:	Government Information (Public Access) Act 2009 (NSW) Health Records and Information Privacy Act 2002 (NSW) Privacy and Personal Information Protection Act 1998 (NSW) Privacy Act 1988 (Cth) Protected Disclosures Act 1994 (NSW) State Records Act 1998 (NSW)

UNIVERSITY OF WOLLONGONG AUSTRALIA

Audience:	Public

Submit your feedback on this policy document using the Policy Feedback Facility.

Contents

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

1 Introduction/Background

1. Data is a key strategic and operational asset of the University and the appropriate governance of the availability, usability, integrity and security of data is critical to the University's operations.
2. This Procedure should be read in conjunction with the IT Acceptable Use Policy, the Data Quality Management Procedure and the Data Handling Guidelines.

2 Purpose/Scope

3. The purpose of this procedure is to:
    a. define the roles and responsibilities for the governance, protection, quality and overall management of data stored by the University;
    b. set the standards for classifying data stored by the University based on its level of sensitivity and value; and
    c. establish principles for creating and maintaining high quality data.
4. This procedure applies primarily to Data Executives, Data Guardians, Data Stewards and the Information Management Unit.
5. Sections 4, 8 and clause 9.1 apply to all Staff.
6. This procedure applies to all data stored by the University, with the exception of data referred to in clause 2.7.
7. This procedure does not apply to:
    a. Research data defined in the Research Data Management Policy; and
    b. data of University controlled entities.
8. The handling of data expressed in this procedure is also underpinned by the University's Data Handling Guidelines, IT Acceptable Use Policy, Privacy Policy, Cyber Security Policy, Records Management Policy and other relevant policies.

3 Definitions

Word/Term	Definition
(Data) Access	The ability to interact with data in one or more ways, such as the ability to read, copy, query, retrieve, update or delete data.
Data	Stored facts and statistics collected for reference, analysis or other purposes as required by University business. Examples of data are provided at Section **7** Data Security Classification.
Data Asset	A structure for grouping data used mainly for practical data management purposes such as access, data security classification, etc. Suggested examples include database column (field), database table, entity, REST API endpoint, source system, etc.

Data Governance	The specification of decision rights and an accountability framework to ensure the appropriate behaviour in the valuation, creation, consumption and control of data.
Data quality	An assessment of data's fitness to serve its purpose in a given context.
Information Governance Committee (IGC)	A university-wide committee, with members consisting mostly of Data Executives, Data Guardians and Data Stewards, whose primary objective is to mandate, advocate and support data as a key strategic asset of the University.
Personal Information	Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion
Sensitive Personal Information	A subset of personal information, defined as: • information or an opinion (that is also personal information) about an individual's: o racial or ethnic origin o political opinions o membership of a political association o religious beliefs or affiliations o philosophical beliefs o membership of a professional or trade association o membership of a trade union o sexual orientation or practices, or o criminal record • health information about an individual • genetic information (that is not otherwise health information) • biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or • biometric templates
Staff	All people employed by the University including conjoint appointments, whether on continuing, permanent, fixed term, casual or cadet or traineeship basis.
University	University of Wollongong.

4 Data Principles

1. Collection, access authorisation, and use of data must be underpinned by a relevant business need.
2. High quality data enables informed decision-making and accurate reporting. The University is committed to the continuous improvement of data quality.
3. The collection and management of Personal Information is to be handled in accordance with the Privacy Policy which facilitates the University's compliance with current legislative requirements.

4. Data stored in University records must be retained and disposed of in an appropriate manner in accordance with the Records Management Policy.

5 Data Governance and Ownership

1. All data assets must have an assigned Data Executive, Data Guardian and Data Steward to ensure clear lines of responsibility and accountability. Data governance roles are defined in the table below.

Role	Definition
Data Executive	Data Executives are members of the Senior Executive Group with strategic planning and decision-making authority for the University's data.
Data Guardian	Data Guardians are senior leadership with high-level knowledge, expertise and tactical decision making in data within their responsibility.
Data Steward	Data Stewards are Staff responsible for data quality, implementation and enforcement of data management within their organisational unit(s).
Data Specialist	Data Specialists are business and technical subject matter experts. They are typically Business or Information Technology specialists who provide ongoing technical support as a part of their day-to-day role.

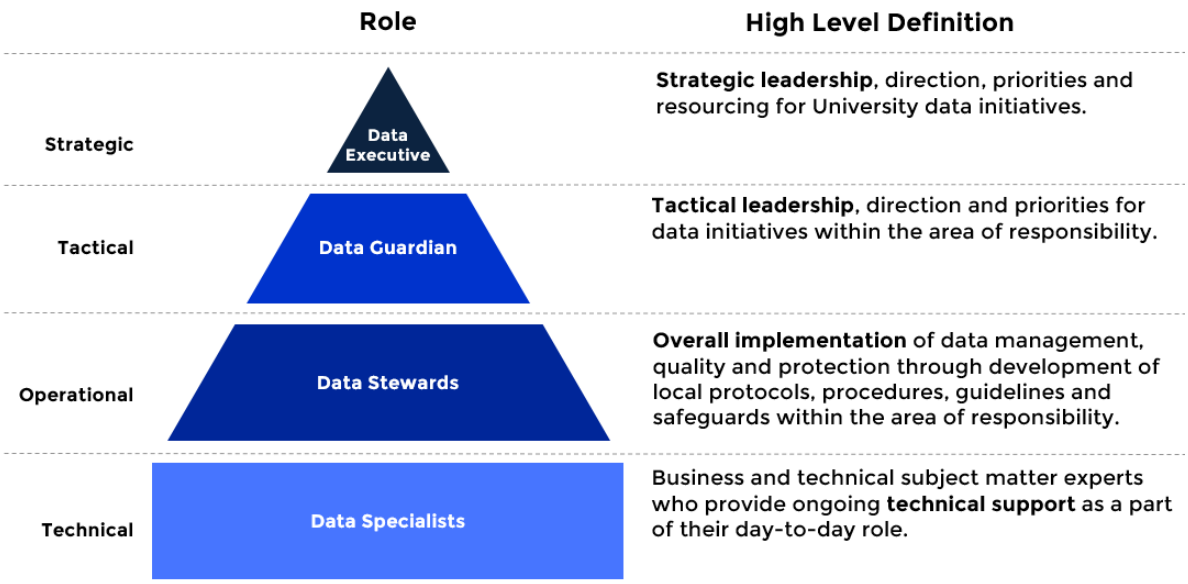

Figure 1 – Hierarchy of Data Governance Roles & Responsibilities

2. Data governance roles are assigned based on the University Enterprise Data Model managed by the Information Management & Technology Services, which separates all University data into information domains and subdomains.

UNIVERSITY OF WOLLONGONG AUSTRALIA

6 Data Quality

1. Data quality requirements must be defined by a Data Guardian, and required data quality monitoring mechanisms put in place.
2. The Data Quality Management Procedure describes the main dimensions used to measure and monitor data quality.
3. Data quality issues must be managed as prescribed in the Data Quality Management Procedure.

7 Data security classification

1. The security classification is based on the likely impact on an individual and/or the University's activities, objectives and reputation resulting from compromise of the data confidentiality.
2. To ensure appropriate handling and protection, University data assets are to be assigned one of the following security classifications.

Classification	Description	Example Data Types
Restricted	Data that if breached due to accidental, negligent or malicious activity would have a high adverse impact on an individual and/or the University's activities, objectives, reputation.	Sensitive Personal Information Personal Information of Children and Young Persons Credit Card information
Protected	Data that if breached due to accidental, negligent or malicious activity would have a moderate adverse impact on an individual and/or the University's activities, objectives, reputation.	Personal Information (such as Student and Staff Data) Assessment and exam data Organisational confidential and financial data
Controlled	Data that if breached due to accidental, negligent or malicious activity would have a low adverse impact on an individual and/or the University's activities, objectives, reputation.	Business processes and procedures Operational records Internal communications which do not contain Protected or Restricted data
Public	Data that if breached owing to accidental or malicious activity would have an insignificant impact on the University's activities and/or objectives.	Web Content Course handbook Published reports Staff directory UOW in Numbers

3. To ensure immediate protection of higher risk data, the ongoing priority for Data Guardians is to identify and classify data assets that should have classification of Restricted.

4. The default security classification for newly created data assets must be Controlled unless there is a specific need to protect the confidentiality of the information. For detailed information on data asset creation refer to the Data Handling Guidelines.

8 Data Handling and Protection

1. The Data Handling Guidelines provide best practice guidance on how to protect and handle data based on security classification of its data assets.
2. Electronically stored data must be protected by appropriate safeguards and/or physical access controls that restrict access to the authorised user(s).
3. Controlled, Protected or Restricted data must not be stored on external portable storage (CDs, DVDs, USB/Flash Drives, etc.), personal devices, personal cloud storage or personal email accounts.
4. Restricted Data must not be stored on University managed devices and should be stored on University managed file servers (Such as H: or S: drives) or with the IMTS approved external services providers.
5. Higher level data assets containing lower level data assets that have different security classification levels must be handled and protected according to the highest security classification assigned to any data asset within.

9 Roles and Responsibilities

All Staff

1. All Staff are responsible for:
    a. complying with this procedure, together with the Data Quality Management Procedure and Data Handling Guidelines;
    b. adhering to the principles laid out in Sections 4 and 8 of this procedure;
    c. handling data based on its security classification level; and
    d. raising data quality issues in accordance with the Data Quality Management Procedure.

Chief Operating Officer

2. The Chief Operating Officer is responsible for appointing Data Guardians on recommendation of the relevant Data Executive.

Data Executive

3. Data Executives are responsible for:
    a. overseeing the continuous improvement of the University's data management, integration and use;
    b. recommending to the Chief Operating Officer the appointment of Data Guardians within their respective portfolio; and
    c. resolving disputes over ownership, access, quality and the classification of data.

Data Guardian

4. Data Guardians are responsible for the overall implementation and enforcement of data management, quality, privacy and security within their assigned domain, including but not limited to:
    a. ensuring that all legal, regulatory, and policy requirements are met in relation to data within their assigned domain;
    b. assigning appropriate security classification levels to data assets;
    c. ensuring that all data assets have a Data Steward(s) assigned;
    d. approving data access requests or establishing an approval model for role-based access to data;
    e. approving the release of University data to be used or shared outside the University;
    f. maintaining acceptable levels of data quality as well as identifying data critical to business operations to be constantly monitored for quality; and
    g. escalating data governance issues to the appropriate Data Executive.

Data Steward

5. Data Stewards are responsible for performing data management, quality, privacy and security tasks as directed by the Data Guardian, as well as:
    a. creating and enforcing processes and procedures for implementation;
    b. acting as subject matter experts for the University community for data within their stewardship;
    c. understanding end-to-end data flows and identifying data dependencies to support enterprise reporting and downstream data consumption;
    d. developing and approving business terms and definitions;
    e. proactively communicating planned changes for data held in systems within their assigned domain;
    f. developing data sharing agreements with other business units;
    g. recommending appropriate data security classifications to the Data Guardian; and
    h. escalating data governance issues to Data Guardian.

The Information Management Unit

6. The Information Management Unit is responsible for:
    a. recording and maintaining the list of the current agreed Data Executives, Data Guardians, Data Stewards and Data Specialists;
    b. locating and assigning Data Specialists;
    c. recording and maintaining the security classification for data assets;
    d. providing guidance for Data Executives, Data Guardians, Data Stewards on the implementation of their duties and responsibilities; and

e. supporting the Information Governance Committee and presenting Data Governance issues and proposals.

The Information Governance Committee

7. The Information Governance Committee is responsible for overseeing the overall implementation of this procedure as prescribed in the Committee's Terms of Reference.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

10 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	9 February 2021	Chief Operating Officer	First Version