Data Governance Policy

Section 1 - Executive Summary

(1) Data comprises the strategic assets of the University of Newcastle (University) as it supports the University's operations and decision making, and ensures the University meets reporting and compliance obligations.

(2) For data to remain useful to the University, it must be handled in a manner that preserves its quality, security and reliability.

(3) All users of the University's data have a role in preserving the quality, security and reliability of University data in line with this Policy.

Section 2 - Purpose

(4) The purpose of this Policy is to:

a. establish roles and responsibilities for data governance;
b. establish the principles for University data governance; and
c. define standards for the quality, security and reliability of University data.

Section 3 - Scope

(5) This Policy applies to all University data, including data of its controlled entities, regardless of its format and including oral data, physical data and electronic data.

(6) This Policy must be applied at all times when engaged in University business or otherwise representing the University.

(7) This Policy is supported by and must be read in conjunction with the following documents:

a. Records Governance Policy;
b. Privacy Policy;
c. Privacy Management Plan;
d. Data Breach Policy (Personal and Health Information);
e. Information Classification and Protection Policy;
f. Information Security Access Control Policy;
g. Digital Technology Conditions of Use Policy;
h. Digital Security Policy;
i. Learning Analytics Policy and Learning Analytics Procedure; and
j. research policies including, but not limited to, Responsible Conduct of Research Policy and Research Data and Primary Materials Management Procedure.

(8) Data may constitute a record, as defined by the Standard on Records Management established under State Records Act. In such cases, the data, as a record, is subject to the requirements of the Records Governance Policy in addition to this Policy.

Section 4 - Audience

(9) This Policy should be read and understood by all University staff, students; University volunteers, contractors and vendors; and members of advisory and governing bodies, in all campuses and locations of the University.

Section 5 - Definitions

(10) In the context of this document, the following definitions apply:

a. “Data” means a set of characters or symbols to which meaning is or could be assigned (As/NZS ISO30300:2020 – Section 3.2.4). The Council of Australasian University Directors of Information Technology (CAUDIT) defines data as a set of facts, representing a specific concept or concepts. Value is added to data when they are combined and presented to users within a context, turning them into meaningful information to support business decisions and enable operational decisions. That is, DATA + CONTEXT = INFORMATION;
b. “Data domain” means a logical grouping of related data assets that represent a specific business function or subject area within the University. Examples include student data, human resources data, finance data and research data. The University has adopted the CAUDIT Higher Education Reference Model (HERM) to define structured data domains, whereby these domains are outlined in the Data Governance Standard;
c. “Data Owner” means a senior business, College , or unit manager who assumes responsibility of data within a specific data domain or dataset;
d. ”Data Steward” means an individual responsible for managing the quality, integrity, and compliance of data within a specific data domain or dataset;
e. “Electronic data” means data created, processed, stored or transmitted in digital form. This includes structured data (for example, databases), unstructured data (for example, documents or emails), and multimedia files;
f. “metadata” means the structured information that describes and provides context for data, enabling the identification, management, accessibility and use;
g. “Oral data” means spoken data captured during University activities, such as interviews, lectures, meetings, or focus groups. When recorded (for example, audio or video), oral data becomes a digital asset and is subject to governance requirements for storage, classification and access;
h. “Physical data” means data represented in a tangible, non-digital format, such as printed documents, handwritten notes, or other hard copy materials;
i. “Record” means any document or other source of information compiled, recorded, or stored in written form, on file, or by electronic process, or in any other manner or by any other means (State Records Act S.3(1) – Definitions). A record, whether digital or physical, is a piece of information that serves as evidence of the University's activities, decisions, and transactions. It is maintained to meet legal, regulatory, fiscal, operational, or historical requirements. Under the Government Information (Public Access) Act 2009 at Schedule 4, S.10 a record means any document or other source of information compiled, recorded or stored in written form or by electronic process, or in any other manner or by any other means. A reference in this Act includes a reference to a copy of the record.
j. “University data” means oral, physical or electronic data that is created, processed, stored, or communicated by the University;

Section 6 - Roles and Responsibilities

(11) All users of University data are responsible for:

a. applying this policy to the data they collect, use and manage on behalf of the University, regardless of location, device or technology used;
b. complying with related policies including but not limited to the Data Breach Policy (Personal and Health Information) and Information Management and Governance Framework;
c. immediately reporting suspected or actual compromise of technologies used to store, process or communicate data to the Cyber Security team. This includes issues or incidents with artificial intelligence (AI) and AI-driven data;
d. reporting data quality issues to the relevant Data Stewards (see Table 1 or roles and responsibilities).

(12) Specialist data governance responsibilities are provided in Table 1.

Table 1 – Specialist Data Governance Responsibilities

Role	Responsibility
Chief Digital & Information Officer (CDIO)	The CDIO is responsible for this policy and oversees the implementation of it across the University. The CDIO is also responsible for data governance practices within Digital Technology Solutions (DTS).
Digital Governance Team	The Digital Governance Team within DTS is responsible for development, implementation, and maintenance of data governance and record governance policies, frameworks and procedures. The team provides subject matter expertise for all University data governance matters. The team maintains the data governance portal, data governance tooling, and develops and implements training resources. The Digital Governance Team identifies Data Owners for assignment to data domains, and provides training for Data Owners where required.
Data Owners	Data Owners are responsible for data within their assigned data domain (e.g. HR, student data). This includes data appropriate collection and use, access, quality and security. Data Owners are endorsed by the Data Governance Committee.
Data Stewards	Data Stewards are responsible for the management of data quality, defining metadata, and implementing the Standards for Data Management (see Section 8) for their assigned data sets. Data Stewards are responsible for conducting regular reviews of data quality and data protections. Data Stewards are identified by Data Owners or System Owners.
Data Governance Committee	The Data Governance Committee (DGC) monitors and guides the implementation of the University's Data Governance Policy. It provides a formal, enterprise-wide governance body that ensures the University's information and data assets are standardised, and are managed responsibly, securely and strategically, aligning with institutional goals and maintaining regulatory compliance. The remit, composition and responsibilities are articulated in the DGC Terms of Reference.

Section 7 - Data Governance Principles

(13) The University upholds the following data governance principles. Data:

a. can be routinely created and captured as part of normal business practice;
b. must be managed in accordance with legal and business requirements, and so that it can be shared as a reliable and trustworthy asset;
c. should be identifiable, retrievable and accessible;
d. must be protected from unauthorised or unlawful access, destruction, loss, deletion or alteration;
e. must be kept for as long as needed for business, legal and accountability requirements;
f. should be systematically and accountably destroyed when legally appropriate to do so.

Section 8 - Standards for Data Management

(14) At a minimum, the following requirements apply to the use of University data.

Ownership

(15) The University requires that all University data has an assigned Information Owner, and that all structured University data should have an assigned Data Owner. Further clarification around ownership roles are defined in the Ownership Role Reference Guide.

Classification and Protection

(16) Data must be classified according to the Information Classification and Protection Policy, State Records Act and its standards, where relevant.

(17) University data must be stored in systems and storage locations approved in accordance with the Digital Security Policy. University research data must be managed in accordance with the Research Data and Primary Materials Management Procedure.

(18) Where data is personal information or sensitive information, data sovereignty requirements must be met, ensuring that University data is stored and processed within jurisdictions that comply with the applicable national and international laws and the University's Privacy Management Plan.

(19) Data must be protected using security controls appropriate to the classification level in accordance with the Information Classification and Protection Policy.

Access

(20) Access to data should only be provided for authorised purposes and to authorised individuals, systems, and services in accordance with the Information Security Access Control Policy. Granting access to a particular data domain is the responsibility of the designated Data Owner as follows:

a. Decisions to grant internal access to data must be documented and auditable, and supported by appropriate mechanisms such as data access agreements or user access approvals. This requirement applies specifically to data accessed for purposes such as system integrations, application workflows, and business intelligence or analytics reporting.
b. This clause does not apply to platform-native sharing capabilities (for example, within Sharepoint or Teams) or to ad-hoc distribution methods such as email, which are governed by separate policies and controls. Note: A staff member may have access to data by virtue of access granted by a System Owner.

(21) Data access agreement guidance can be provided by the Digital Governance Team.

(22) University data must not be shared with external parties unless in accordance with a legally binding agreement that is approved by an authorised delegate and stipulates conditions for use, handling and protection. The sharing of University research data must be in line with the Research Data Management Plan.

Cataloguing and Consistency

(23) Data assets should be catalogued for visibility and discovery.

(24) Data assets should have consistent definitions.

(25) Data should not be duplicated across systems, platforms, devices and storage locations unless required for

business reasons.

Legal and Ethical Compliance

(26) Data must be handled in accordance with relevant University policies and applicable national and international laws.

(27) Data collection, use, handling and transformation should be ethical in all contexts and free from bias wherever possible.

Data Quality and Lifecycle Management

(28) Data must be maintained throughout its lifecycle which spans collection, storage, access, usage, archiving, and disposal.

(29) Data quality standards are defined and reflect the value, purpose and usage of data.

(30) Data must be subject to regular quality reviews.

Emerging Technologies and Artificial Intelligence (AI)

(31) The use of University data in emerging technologies and AI must be in accordance with relevant University policies and procedures and applicable laws.

(32) Any application of AI-powered systems for the management of data must include documentation of methodologies and auditability features.

User Awareness

(33) Staff should be provided with regular data management training to support awareness of data governance policies and procedures.

Section 9 - Enforcement

(34) Non-compliance with the provisions of this Policy may result in action under the University's policies, delegations, Staff Code of Conduct, Student code of Conduct or the relevant enterprise agreement/employment contract, and may also result in referral to a statutory authority and/or agency.

Section 10 - Relaxing Provision

(35) To provide for exceptional circumstances in any case, the Chief Digital & Information Officer may relax any provision of this policy, provided that the relaxation:

a. does not compromise compliance with external obligations (including but not limited to contractual, legislative, or accreditation requirements);
b. does not override a decision made under a formal delegation of authority; and
c. does not replace a decision that is subject to a formal delegation of authority.

(36) A relaxation may be requested in writing to the Digital Governance Team and will be assessed based on the potential business impact, the security risk that the proposed relaxation may pose, and any compensation controls that may be implemented in relation to the relaxation.

Status and Details

Status	Current
Effective Date	28th May 2026
Review Date	16th April 2029
Approval Authority	Senior Compliance Manager
Approval Date	27th May 2026
Expiry Date	Not Applicable
Responsible Executive	Anthony Molinia Chief Digital & Information Officer +61 49138713
Enquiries Contact	Digital Governance Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Asset" - Any tangible or intangible item (or group of items) that the University owns or has a legal or other right to control and exploit to obtain financial or other economic benefits.

"Controlled entity" - Has the same meaning as in section 16A of the University of Newcastle Act 1989.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Information Owner" - A senior business, college or unit manager whom the University has authorised to collect, create, retain and maintain information within their assigned area of control.

"Research" - As defined in the Australian Code for the Responsible Conduct of Research, or any replacing Code or document.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"System Owner" - An authorised individual who has been allocated responsibility by the University and is held accountable for an ICT resource.

"University business" - Work that the University has directed to be undertaken which is required, essential, and beneficial for the functions of the University. This includes, but is not limited to, attending meetings, conferences or fieldwork, but does not include activity that is not location specific, e.g. email management, writing papers. University business may be undertaken by staff and non-staff.

"Delegate" - (noun) refers to a person occupying a position that has been granted or sub-delegated a delegation of authority, or a committee or body that has been granted or sub-delegated a delegation of authority.

This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to the Policy Library for the latest version.