Information Governance and Management Framework

Section 1 - About this Document

Executive Summary

(1) The Information Governance and Management Framework (the Framework, this Framework) establishes the University of Newcastle's (the University) overarching approach to governance and management of University information, including data and records.

Purpose

(2) The Framework defines the University's information governance and management roles, authorities, and structures to describe our approach to information management to meet current and future organisational needs and regulatory requirements. It includes all the University's information, including data and all files and records to:

a. support strategic objectives.
b. ensure University information is protected and preserved.
c. enable effective, ethical and secure use of University information; and
d. meet legislative and administrative obligations.

(3) This document should be read in conjunction with the policies listed in Section 8.

Scope

(4) The Framework applies to all University information, data and records (as defined by this Framework), excluding information generated by individuals listed below (See: Audience) as part of a program of studies or whilst attending an event.

Audience

(5) Individuals who use, create or access University information must comply with this Framework. This includes, but it is not limited to, all University staff (including those employed by a controlled entity), contractors, third party providers and affiliates who are authorised to access and use University information.

Definitions

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

Defined Term	Meaning
Data	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.

Defined Term	Meaning
Data asset	An individual unit of data that holds value and may include files, databases, documents, websites, physical records, learning materials, web pages, videos, audio recordings, and assessment materials (ASC).
Data management	Activities involved with managing data across the full lifecycle so that it is protected from unauthorised use and inappropriate deletion. Data needs to be appropriately managed from procurement or service design through to creation and final disposal. This includes protection of personal, health and sensitive information, and the prevention of deletion until enabled by legal authorisation. (See NSW Government Data Glossary).
Information	Data in context with a particular meaning (AS/NZS ISO 30300:2020 – Section 3.4.7). Information is data that has been organised, or structured, or processed, in a way that it now has meaningful context and can be understood and interpreted by people or systems. Information is data that has been given significance through relational connection, analysis, or interpretation, turning it into a valuable resource. (USC)
Information domain	A concept for information sharing, independent of, and across information systems and security domains, including: i. identification of information sharing participants as individual members; ii. shared information objects; and iii. linked to a security policy that identifies the roles and privileges of the members and the protections required for the information objects (NIST).
Information entity / information entities	Groups of information related to an information domain.
Information Management	Planning, collection, control, distribution and exploitation of information resources within an organisation, including systems development, and disposal or long-term preservation (AS ISO 5127:2017 – Clause 3.2.1.23).
Record	Record means any document or other source of information compiled, recorded or stored in written form or on film, 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.
Recordkeeping	The process of making accurate and reliable records and capturing them in the University's official recordkeeping systems.
Records management	A field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition (disposal) of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records (AS ISO 15489.1:2017 – Clause 13.15). (State Records, NSW).
Senior responsible officer (SRO)	The Senior Responsible Officer (SRO) is the individual within the public office who has been delegated strategic and corporate responsibility for records and information management. The SRO is usually a senior manager reporting to the Chief Executive or to the Chief Information Officer. At the University of Newcastle, the University Secretary is the SRO with a responsibility for ensuring that records and information management is in place and operating effectively to support business operations. (State Records, NSW).
State archive	State archive means a state record that Museums of History NSW has control of under the State Records Act. (State Records Act, 2.3 (1) – Definitions).
State record	State records means a record made or received by a person: i. while exercising official functions in a public office, or ii. for a purpose of a public office, or iii. for the use of a public office. (State Records Act, 1998, S.3(1) Definitions).
University information	University information refers to data, information, and records, including: i. records, as defined by the State Records Act, 1998 (NSW). ii. active, semi-active and archived information assets. iii. information assets classed as State archives. iv. structured and unstructured information. v. data assets (physical and digital); and vi. research data hosted on-campus or externally with third party vendors.

Section 2 - Principles

(7) The below principles outline the core characteristics of information governance at the University. University information is integral to its operations and effectiveness.

Principle 1: Information is business enabling, aligned to our functions and supports informed decision making

(8) Information is designed and managed so that it directly supports the University to meet its obligations. We strive to deliver data analyses, dashboards, reports, and visualisations for information and data-driven decision making.

Principle 2: Information is secure, valued, and managed as an asset

(9) Information is a core component of the University services and operations, and it is supported and maintained as a secure, long-term business asset in accordance with approved authorities.

(10) On behalf of the Museums of History NSW, we are a custodian of the information about the University and our community. This information is both digital and analogue, and we create policies, plans and processes to realise and protect these assets. We describe and register our information assets and ensure each asset has an authorised custodian.

Principle 3: Information is trustworthy, used and reused with confidence

(11) Information is accurate, authentic and trusted, allowing its ongoing use and reuse by government and our community.

Principle 4: Information is High quality

(12) Quality information is essential to meet our strategic objectives, and when appropriate, it will be used for improved service planning and delivery, and business performance insights.

(13) We implement innovative processes, tools, and technologies to enhance consistency, efficiency, capability, authority and quality of information.

Principle 5: Information is managed across the full lifecycle, protected from unauthorised use and inappropriate deletion.

(14) Information is appropriately managed from procurement and service design, through creation, storage and to final disposition. This includes the protection of personal, health and sensitive information, and prevention of deletion until enabled by legal destruction authorisation.

Principle 6: Information is available and open to the community and government.

(15) University information is discoverable and used by those with a legitimate need. We promote accessibility through appropriate access, formats, and metadata, and through interoperability as needed across systems, channels, and technologies.

(16) Information often has a lifespan longer than the technology on which it is hosted, therefore information is considered as a separate entity to technology and governed in accordance with its value and risk.

Principle 7: Leadership

(17) Our leaders recognise their information management responsibilities and understand that the value of

information captured in University systems and activities. There is a commitment to ensure that information management is appropriately resourced and supported through strategies, policies, guidance and procedures, along with information governance education and training.

Principle 8: Capture

(18) The capture of information in approved information management systems is essential for managing its use and access over time. Fit for purpose information storage will allow creation of information assets to inform, implement, document, and communicate our activities and decisions, promoting the ability to work cohesively and provide accessibility.

Section 3 - Information Governance

(19) University information governance defines the roles and responsibilities, decision rights, controls, and processes used to manage University information.

Information Classification

(20) University information is grouped according to Information Domains based on the CAUDIT Higher Education Data Reference Model. Each Information Domain is assigned to an Information Domain Custodian and Information Leader (who oversees a group of domains based on organisational structures). For more information, view the Enterprise Configuration Database and Governance Policy, Information Security Access Control Policy and Information Classification and Protection Policy.

Information Governance Committee

(21) The Information Governance (IG) Committee provides advice and recommendations for strategy, policy and risk related matters impact on the University's Information. The membership, roles and responsibilities of the IG Committee are codified in its Terms of Reference.

Artificial Intelligence

(22) The University has adopted several Artificial Intelligence (AI) platforms and technologies and implemented policies to support academic integrity and ethical usage in teaching and research. The University recognises the efficiencies and innovation AI offers and they are implemented in a secure and ethical manner in accordance with the Digital Technology Conditions of Use Policy. The University is committed to following the principles laid out in the National Framework for the assurance of AI in government to ensure any use we make of AI is safe and responsible.

Information Systems Governance

(23) University information is:

a. retained in various business applications and storage systems across the University; and/or
b. stored in both On-Premises and Cloud based repositories.

(24) Digital Technology Solutions (DTS) is responsible for:

a. managing records of business system applications, including data sensitivity and business criticality designations;
b. determining data sensitivity and business criticality designations through a structured process in collaboration with system owners and in accordance with the Information Classification and Protection Policy and Business Continuity Management Framework;

c. maintaining records of system owners and information service providers;
d. assessing and reviewing new applications and systems during the design stage and prior to deployment to ensure appropriate security considerations have been included in accordance with the Digital Governance Framework.

(25) Records Governance Services is responsible for:

a. maintaining a Record and Information Asset Register (in consultation with DTS).

Risk Mitigation

(26) Consideration of risk is a key component underlying this framework. University information is subject to internal and external audits to:

a. assess integrity and performance of specific information management processes, services or environments; and
b. monitor adherence to mandatory legislative obligations including information creation and retention, information access, or privacy protections for personal information and health information.

(27) The major risks for the University's information assets are identified in the Record and Information Asset Register.

(28) The following operational measures also serve as risk mitigation strategies:

a. Information Governance Committee.
b. Records Governance Services business responsibilities for the University records management program, including the Business System Recordkeeping Assessment Checklist used as a validation tool to assess all new business systems and review existing systems.
c. Assurance activities and annual reporting surveys to ensure the University is accountable and meeting its information requirements.
d. Cyber security controls aligned with the NIST Cyber Security Framework (CSF).
e. Business Continuity planning / testing.

Section 4 - Information Management

Information Lifecycle Management

(29) Management of University information drives improvements in performance and infrastructure costs and influences how the University manages information. For all University information, the lifecycle management process should include the following phases, commensurate with the value of the University information:

a. Plan and design: University information management should be carefully planned, with management activities designed to meet University needs and compliance requirements throughout the lifecycle.
b. Create, capture and classify: University information may be obtained through several means including manual data entry and automatic capture via devices or systems. At the time information is acquired, key metadata should be recorded, including the information security classification.
c. Store and secure: University information must be stored appropriately, with consideration given to security and access management.
d. Manage and maintain: University information management is an active process. Information should be managed to maintain its integrity, quality and usability.
e. Share and (re)use: Sharing and re-use of University information requires oversight to ensure it is ethical and

compliant with University policies and legislative requirements. Information should be discoverable to streamline sharing and re-use for appropriate activities.

f. Retain and archive: University Information should be retained while required and archived in line with any relevant record retention periods.
g. Dispose or destroy: University information should be destroyed in an appropriate manner at the end of its useful life, ensuring that records are destroyed (or transferred to the appropriate owner) in line with Records Governance Policy.

Section 5 - Roles and Responsibilities

(30) The Vice-Chancellor has University-wide authority and accountability under legislation for the compliant collection and management of the University's information and may sub-delegate these responsibilities to other roles in accordance with the Governance Rule.

(31) The Chief Digital & Information Officer (CDIO) is responsible for the management of the technical and specialist teams relevant to information governance and for oversight of the infrastructure framework for the management of information and the University's IT Security Programs.

(32) The University Secretary is the Senior Responsible Officer (SRO) under the State Records Act 1998.

(33) Individuals, as defined in Audience of this Framework and as it relates to information that they create, manage or use, are responsible for:

a. fulfilling the responsibilities as an information owner,system owner and/or system administrator as dictated by University policy;
b. controlling and safeguarding University information;
c. ensuring quality and integrity of information by embedding information governance and compliance processes into daily operations and systems;
d. capturing or creating University information; and
e. selecting the best source of information to meet a specific use-case and defining criteria of what makes information fit for purpose.

(34) The Information Governance Specialist based Digital Technology Services (IT Governance), , Risk, Business Continuity, Legal and Compliance, Research Integrity Unit, and subject matter experts from across the university.

(35) Records Governance Services responsibilities are codified in the Records Governance Policy.

(36) The Privacy and Rights to Information Manager responsibilities are codified in the Privacy Management Plan and the Privacy Policy.

(37) Governance and Management Committees:

a. The University's governance includes Council, Risk Committee, Academic Senate and its committees. The Vice-Chancellor maintains the Executive Leadership Team as an advisory body on matters of strategy and operations.
b. The Chief Operating Officer maintains various committees supporting digital technology services and library services.

Section 6 - Compliance Requirements

(38) Compliance with this Framework is important in protecting the University's information. Breaches may be reported via the University Breach Register. Non-compliance may result in proceedings in accordance with an employment contract, or Enterprise Agreement or the Staff Code of Conduct.

Section 7 - References

(39) The following information sources have been referenced in developing this Framework:

a. Australian National Audit Office – Audit Lessons Insights – Records Management (2025)
b. Australian Government Office of the National Data Commissioner – The Foundational Four.
c. NSW Information Management Framework.
d. University of Newcastle Act, 1989.
e. State Records Act, 1998.
f. National Archives of Australia – Information and Data Governance Framework (2024).

Section 8 - Supporting Documents

(40) Art & Special Collections Management Framework

(41) Copyright Compliance Policy

(42) Complaint Management Procedure

(43) Cyber Security Incident Management Procedure

(44) Data Breach Policy (Personal and Health Information)

(45) Data Governance Policy.

(46) Digital Security Policy

(47) Information Classification and Protection Policy

(48) Information Security Access Control Policy

(49) Privacy Policy

(50) Privacy Management Plan

(51) Records Governance Policy

(52) Responsible Conduct of Research Policy.

(53) Research Data and Primary Materials Management Procedure.

Status and Details

Status	Not Yet Approved
Effective Date	To Be Advised
Review Date	To Be Advised
Approval Authority	
Approval Date	To Be Advised
Expiry Date	Not Applicable
Responsible Executive	Dianne Allen University Secretary dianne.allen@newcastle.edu.au
Enquiries Contact	Governance and Assurance Services

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.

"Campus" - means any place or premises owned or controlled by the University, but may also specifically refer to a designated operating location such as the Callaghan Campus.

"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).

"Health information" - As defined in the Health Records and Information Privacy Act 2002, or any replacing legislation.

"Information asset" - A body of information, knowledge or data that is organised as a single entity and has value to the University.

"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.

"Program" - When referring to learning, a program is a sequence of approved learning, usually leading to an Award. For all other uses of this term, the generic definition applies.

"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.

"Affiliate" - A person or organisation legally obligated to, or informally associated with the University. Categories of affiliates are outlined on the University website.

"System Administrator" - An individual responsible for the installation and maintenance of an information system, providing effective information system utilisation, adequate security parameters, and sound implementation of established Information Security policy and procedures.