Records and Information Management Policy

Section 1 - Audience

(1) This policy applies to all University staff, contractors, volunteers, students, work experience participants, members of advisory and governing bodies as well as staff of controlled entities of the University.

Section 2 - Executive Summary

(2) The University of Newcastle's (University) records, information and data provide evidence of teaching, research and administration and are a critical asset to the University. They provide the foundation to support business activity, decision making, document rights and entitlements, make up the corporate memory, drive collaboration and communication, preserve knowledge, and provide stakeholders with transparency and accountability for University operations.

(3) Having the capacity to strategically plan, readily identify, securely store and manage records, information and data is essential to the efficient and effective operation of the University.

(4) The University has responsibilities for record, information and data management as per the State Records Act 1998 (NSW), as well as reporting responsibilities to the State Records NSW in accordance with the objectives outlined in their Regulatory Framework (2021-2024). This Framework includes mandatory annual self-monitoring activities for the University to assess how they comply with the State Records Act 1998 and relevant standards that are legislated under the Act.

(5) The University is also obligated under a range of legislation to maintain appropriate records, reproduce records, or retrieve documents. This includes, but is not limited to:

a. Independent Commission Against Corruption Act 1988 No 35;
b. Public Interest Disclosures Act 2022;
c. Tertiary Education Quality and Standards Agency Act 2011;
d. Work Health and Safety Regulation 2017;
e. Evidence Act 1995;
f. Electronic Transactions Act 2000;
g. Government Sector Audit Act 1983;
h. Government Information (Public Access) Act 2009
i. Privacy and Personal Information Protection Act 1998 No 133; and
j. Health Records and Information Privacy Act 2002 No 71.

Section 3 - Purpose

(6) This policy identifies how the University will meet its obligations under the State Records Act 1998 (NSW), the principles of the Standard No 12: Standards on Records Management, State Records Regulations 2015, and State Records NSW Regulatory Framework (2021 -2024). This policy outlines how the University will govern the

management and minimise risk relating to records, information and data and preserve assets of corporate and community significance.

Section 4 - Scope

(7) This policy applies to records, information and data in any format that is created, received or maintained by the University, and that documents research, deliberation, advice or actions undertaken in the course of carrying out a University function or activity (called herein 'University Records').

(8) This policy does not apply to University records that:

a. can be destroyed in accordance with the Normal Administrative Practice (NAP) provision;
b. are classified as State Archives and are under the current control of State Archives in the University's Special Collections unit. These records are bound by the Art and Special Collections Management Framework; or
c. are created and retained at the University of Newcastle Singapore (UONS) campus and are not under the control of the University of Newcastle, unless stipulated in a UONS agreement or constitution.

Section 5 - Policy Specific Definitions

(9) In the context of this policy:

a. "high risk records" means those University records, information and data that are created in high-risk business processes or functions or received in high risk areas of the business that would be considered at a level of risk that is outside the University's risk appetite if they were misused, released inappropriately, or inappropriately accessed and altered, lost damaged or destroyed prematurely;
b. "high value records" means those University records, information and data that enable the University to continue their functions, provide a service, and respond to Royal Commissions, inquiries, audits, investigations and legal issues;
c. "University function or activity" means any decision, action, or risk assessment undertaken by or on behalf of the University to further its statutory objectives, including but not limited to research, research administration, teaching, strategic and business planning, ensuring health and safety, student administration, alumni administration, human resource management, financial management, governance and administration of the University, and commercial activities;
d. "University records" refers to physical and digital records that are created whilst performing a University function or activity, including but not limited to paper based records; databases; emails; scanned documents; records created in collaboration sites such as (but not limited to) MS365-Teams, Sharepoint, document libraries and OneDrive; completed on-line forms; actioned workflows; records created in cloud based third party applications; microfilm; tape; photos; video footage; webpages; social media content; maps; and research data;
e. "State Archives" means those University records that are appraised by the University in accordance with the statutory framework as having historical, long term continuing value, and that the State Records Authority has control of under the State Records Act 1998. Examples of State Archives include, but are not limited to:
    i. master sets of by-laws, rules, and policies;
    ii. master sets of Senate, Council, Health and Safety and similar governing bodies meeting papers;
    iii. annual reports;
    iv. registers of graduates, scholarships, and final academic transcripts;
    v. final approved curricula;
    vi. records of ownership of intellectual property;

vii. research project final reports; and
viii. strategic plans;

f. “disposal” refers to processes and decisions associated with record and information retention, destruction or transfer which are documented in disposal authorities;
g. “University Records Management System” is an approved information system that has the capability to compliantly manage records. This system (TRIM) is controlled by Records Governance Services;
h. “University Approved Information Systems” are systems supported by the University that have been assessed by Records Governance Services for suitable record keeping functionality, and Digital Technology Solutions for acceptable security functionality. Refer to Information Security Policy for more information;
i. “data subjects” under the General Data Protection Regulation (GDPR) is anyone within the borders of the European Union (EU) at the time of processing of their personal information;
j. “records management” refers to the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including people, processes, and systems used to capture and maintain evidence of and information about business activities and transactions in the form of records;
k. “retention period” refers to the minimum period of time for which records should be kept to meet regulatory, business, audit, legal and financial requirements before they can be destroyed;
l. “Normal Administrative Practice (NAP)” refers to the provision under the State Records Regulation 2015 to routinely destroy certain types of facilitative and duplicate records that have limited or incidental relevance to the performance of a University function and are usually not required for on-going business or accountability purposes. Examples include:
    i. working papers that are primarily facilitative, and the capture of the final version will meet business, accountability, and recordkeeping requirements;
    ii. drafts that are routine in nature and do not contain significant information or document significant decisions, discussions, reasons, and actions and are not intended for further use or reference;
    iii. facilitative records that do not provide continuing value and are routine in nature;
    iv. computer support records that do not support significant functions or required for ongoing business purposes;
    v. published or reference material; and
    vi. personal emails not relating to University functions or activities.
m. “Access Directions” refers to the framework for regulating public access to State records which have been in existence for at least 30 years (the ‘open access period’). Records can be subjected to open public access (OPA) or closed public access (CPA) directions;
n. “Information Users” refers to individuals who have been granted explicit authorisation by the relevant Information Owner to access, use, alter, or destroy information within a University approved information system;
o. “sentencing” refers to the process of classifying records to determine how long they need to be kept and in accordance with the disposal authorities. Sentencing ordinarily takes place upon creation of a record; and
p. “inactive records” refers to those records that are not required to meet immediate business needs, but which must be kept (in accordance with retention and disposal authorisation) to support business activities, legal or regulatory requirements, or societal expectations.

Section 6 - Principles

University Records and Information Management Program

(10) The University's records and information management program will satisfy the requirements of the State Records Act 1998 NSW, and any associated standards, policies and guidelines.

(11) The program, including policies, procedures, people, and systems required to manage University records will be monitored and evaluated for risk management, continuous improvement, and assurance that the needs of the University, community and the regulatory requirements are met.

Ownership, control and custody of University Records

(12) All University records created or received while performing a University function or activity are owned by the University, unless otherwise specified under contract, and must be managed in accordance with this policy.

Creation and Management of University Records

(13) Information Owners must:

a. assess, document and review the University records that will be created and captured as part of a process that they are responsible for, and determine how long these University records need to be kept to meet the requirements of this policy;
b. ensure that the University records they are responsible for are reliable, accurate, usable, stored and appropriately protected within a University Approved Information System or a compliant storage area (for physical records); and
c. ensure sensitive, personal, and confidential University records are:
    i. protected against unauthorised access;
    ii. not kept for any longer than necessary; and
    iii. destroyed in line with the relevant disposal authorities.

(14) Prior to entering into arrangements with third party providers to store and manage University records outside of NSW, an evaluation must occur in line with State Records NSW – General Retention and Disposal Authority GA35 - Transferring Records out of NSW to determine and mitigate risks associated with storing University records outside NSW jurisidictions.

(15) Email folders, shared drives, personal drives, external storage media or unsupported cloud-based storage services (e.g. drop-box) must not be used to store University records as these lack the necessary record-keeping functionality to protect the records. University records held in these systems must be incorporated into the University's Approved Information System to prevent them from being inaccessible, lost, leaked, prematurely deleted or over-retained. Records with a high or medium risk rating (refer to the "Records and Information Risk Assessment Guide") must be stored in the approved University's Records Management System.

Retention and Disposal of University Records

(16) Retention periods for University records are set by the State Records NSW in the State Records NSW - Retention and Disposal Authorities. Disposal Authorities are legislated under the State Records Act 1998 (NSW) and take into account the needs of the business, legal and accountability requirements, and community expectations.

(17) The University uses a number of General and Functional Disposal Authorities to manage retention requirements of University records. University records must be sentenced according to the disposal authorities when the records are created, or prior to the records being disposed of or destroyed.

(18) University records that are inactive and no longer required to meet immediate business needs but are required to be retained until they have met the minimum retention requirements, can be moved to approved semi-active or long-term storage repositories.

(19) Destruction of University Records prior to completion of the minimum retention period is prohibited under the State Records Act 1998 (NSW) which also prescribes penalties and exceptions for early destruction. Records having

limited or incidental relevance can be destroyed in accordance with Normal Administrative Practice (NAP).

(20) Destruction of University records must be authorised, secure, timely and documented to minimise risks associated with records being accessible beyond their requirements; to reduce costs associated with record storage; and comply with the State Records Act 1998 and Privacy Legislation.

(21) Destruction of paper based records after they have been scanned/digitised is acceptable providing the conditions outlined in the State Records NSW - General Retention and Disposal Authority GA45 - Original or source records that have been copied are met, and the digital outputs are stored in a University Approved Information System.

(22) Destruction of digital records must be in accordance with the State Records NSW - Destruction of Records Guideline and must include:

a. the date of the destruction;
b. identification of who/what undertook the destruction;
c. the disposal authority reference for the destruction (e.g. GA27 1.2.3; By Court Order); and
d. the title of the record or identifier (e.g. student, staff or client/partner name).

(23) The Vice-Chancellor has sub-delegated the authority for approving the destruction of records and information (please see Delegations Register). The destruction authorisation process is managed by Records Governance Services.

University Records and Information Management Systems

(24) Information Owners must consult with Records Governance Services prior to implementing new or upgrading existing University Approved Information Systems to ensure record management requirements and obligations can continue to be met. In particular, information systems that capture and store high value records and high risk records must comply with the requirements of the State Records NSW Standard No 12 Standard on Records Management or be linked to the approved University Records Management System (TRIM).

(25) University Approved Information Systems must include minimum metadata requirements to support identification, usability, accessibility and context of University records in accordance with Standard No 12: Standard on Records Management.

(26) System Owners and System Administrators must ensure that appropriate design and maintenance documentation is developed to assist with monitoring, auditing, and ensuring records and information management systems operate as expected.

Access to University Records

(27) Information Owners and System Administrators must ensure that the University records for which they are responsible for are protected from unauthorised access, disclosure, modification, loss, or damage. Particular attention must be given to restricting access and securing sensitive, personal, health, and confidential records and information.

(28) Information Owners must periodically review access to systems that they are responsible for to ensure information user's access is relevant, and to remove information user's access to systems when it is no longer required.

(29) The Information Security Policy, Privacy Policy and Privacy Management Plan and their associated documents must be complied with when accessing records and information.

(30) Access to research data/primary material must follow the Research Data and Primary Materials Management Procedure.

(31) Access to University records that are not made publicly available by the University may be provided to external parties if authorised by the information owner and considered permissible under all relevant University policies, or where required by law.

(32) The information owner is responsible for ensuring that the University records they are responsible for and that are older than 30 years are subject to Access Directions based on Museums of History NSW - Attorney General's Guidelines for making access directions. Closed Public Access (CPA) directions means all records are closed to public access until the record reaches a certain age. Open Public Access (OPA) directions provides public access to records once the record is 30 years old.

Security of University Records

(33) University Approved Information Systems must meet the requirements of the University's Information Technology Security policies, procedures, guidelines, and manuals so that the University records are protected and available wherever they are located.

(34) Security classifications must be applied to all University records in accordance with the Data Classification and Handling Policy and Standard. Security classifications are based on sensitivity, risk and potential impact on the University in the event that the records or information is disclosed, misused, misinterpreted or lost.

(35) Physical University Records must be stored securely and have appropriate environmental controls in place, consistent with Standard 11: Standard on Physical Storage of State Records.

(36) System Owners and System Administrators must ensure the implementation of established information security policy and procedures, in the system they are responsible for. For more information please refer to the Information Security Policy.

Out-sourcing University Records

(37) Information Owners must assess out-sourced information systems prior to their use to ensure recordkeeping requirements meet the requirements of Standard No 12: Standard on Records Management and risk management meets the requirements of the University's Risk Management Framework.

(38) Records that have the potential to be classified as State Archives that are older than 25 years must not be stored outside NSW without first seeking the approval of Records Governance Services.

(39) Physical records must not be stored with off-site storage providers other than with the current University contractor. Records Governance Services are the single point of contact for the University off-site record storage contractor.

State Archives - Transfer of University Records

(40) Digital State Archives must be migrated to the University's Records Management System in a suitable long-term format once they are inactive and no longer required for business legal or audit purposes (Please see State Records NSW - Digital Records Preservation Policy). Digital State Archives must be transferred to State Records NSW when they are at least 25 years old.

Decommissioning and Migration of IT Systems and Data

(41) Decommissioning of information systems and legacy data must be planned and documented, and the plan must comply with the retention and disposal requirements outlined in the State Records NSW - Retention and Disposal Authorities.

(42) Migration and conversion processes must be planned, documented, and tested to ensure that the University

records that are migrated and/or converted remain accurate, reliable, and useable, and that metadata remains associated with the records. (Please see State Records NSW - General Retention and Disposal Authority GA48 - Source records that have been migrated).

Risk and Business Continuity

(43) The University will ensure its Business Continuity Plans for critical processes identify the risks to high risk records and high value records, and will implement processes to monitor and manage these risks in line with the University's Business Continuity Management Framework. This includes, but is not limited to, appropriate back-ups and disaster recovery strategies.

(44) Information Owners must follow the Records and Information Risk Assessment Guide to determine the level of risk associated with the records that they are responsible for and apply a risk-based approach when considering the best way to manage and store records.

(45) High risk records and high value records must have more rigorous records management processes applied, whereas low risk and low value records have more flexibility in their record management provided that key recordkeeping and privacy obligations are met.

(46) Staff must plan and facilitate the transition of records to the most appropriate person or business unit to minimise disruption of operations and loss of information prior to a staff member leaving the University, moving divisions, business units, or premises; or when there is a restructure.

Monitoring

(47) Regular assessment of the effectiveness and efficiencies of recordkeeping processes is required to ensure that they support the functions and activities of the University as well as compliance requirements. This may include, but is not limited to:

a. benchmarking against Standard No 12 – Standards on Records Management using the Records Management Assessment Tool (RMAT);
b. assessment against plans, goals and objectives of the business unit records management program;
c. auditing of recordkeeping and/or management of records;
d. conducting detailed reviews of high-risk business areas to confirm that records are being created and captured into the recordkeeping system;
e. assessing compliance against the State Records Act 1998; and
f. assessing records management system and business systems that create and capture records.

General Data Protection Regulation – GDPR

(48) University records relating to data subjects within the European Union (EU) and related to University core functions or activities are to be retained with the State Records Act 1998 (NSW).

(49) Requests to alter personal information in University records must be undertaken in accordance with the University's Privacy Management Plan.

Section 7 - Roles and Responsibilities

All staff

(50) All staff are responsible for the management of University records in accordance with this policy. All new staff to

the University must complete the relevant on-line record-keeping training which details the record-keeping requirements for the University. Additional responsibilities for certain staff are listed below.

Vice-Chancellor

(51) The Vice-Chancellor is responsible for ensuring the overall management of University records complies with the requirements of the State Records Act 1998 (NSW).

Senior Staff

(52) Senior staff are responsible for ensuring adherence to this policy by supporting and implementing comprehensive records management programs and promoting a culture of compliance records management that meets the requirements of the University and its stakeholders.

Senior Responsible Officer

(53) The University Secretary is the senior responsible officer, as required by State Records NSW, and has oversight of records and information management at the University.

Records Governance Services

(54) Records Governance Services is responsible for overseeing the management of University records at the University, consistent with the requirements described in the policy, including the provision of advice, training, approving the disposal of University records, and the assessment of proposed new and existing information systems.

Chief Digital & Information Officer

(55) The Chief Digital & Information Officer is responsible for maintaining the technology for the University's information systems in accordance with State Records legislation and this policy. This includes routine testing or audit of systems to ensure that there are no issues affecting information integrity, usability, confidentiality or accessibility.

Managers and Supervisors

(56) Staff who have responsibility for the management or supervision of divisions, units, teams or other employees are responsible for ensuring they maintain a detailed understanding of this policy, that records and information management are integrated into work processes and systems, and that their staff (including contract staff), are aware of and are supported to follow the requirements of this policy.

Information Owners

(57) Information Owners must ensure that record management requirements are identified and managed and that the development and implementation of any new University Approved Information Systems that they are responsible for are managed in accordance with this policy.

System Owners and System Administrators

(58) System Owners and System Administrators must ensure that the systems they are responsible for meet the requirements of Standard No 12: Standard of Records Management and configuration and system design documents are relevant and up-to-date.

Contract Owners of Managed Service Providers

(59) Staff responsible for the approval of the procurement of IT managed services must ensure that suitable contract

provisions require the provider to comply with the provisions of this policy. Contract owners, as defined by the Procurement Policy, must ensure compliance by the provider throughout the contract term.

Status and Details

Status	Historic
Effective Date	24th May 2023
Review Date	29th June 2023
Approval Authority	University Secretary
Approval Date	24th May 2023
Expiry Date	28th November 2023
Responsible Executive	Daniel Bell University Secretary
Enquiries Contact	Nerida Lithgow Manager, Records Governance Services Legal and Governance Services

Glossary Terms and Definitions

"Graduate" - (Noun) Has the same meaning as in section 3(2) of the University of Newcastle Act 1989.

"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.

"Risk management" - The co-ordination of activities to optimise the management of potential opportunities and reduce the consequence or impact of adverse effects or events.

"Risk assessment" - The overall process of risk identification, risk analysis, and risk evaluation.

"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.

"Intellectual property" - Intellectual property (IP), as defined by the World Intellectual Property Organisation, refers to creations of the mind: inventions; literary and artistic works; and symbols, names and images used in commerce. Intellectual property is divided into two categories: Industrial property includes patents for inventions, trademarks, industrial designs and geographical indications; and Copyright covers literary works (such as novels, poems and plays), films, music, artistic works (e.g. drawings, paintings, photographs and sculptures) and architectural design. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and broadcasters in their radio and television programs.

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

"Senior staff" - Deputy Vice-Chancellor, Pro Vice-Chancellor, Global Innovation Chair, Global Innovation Professorial Fellow, Head of School, Director or equivalent.

"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.

"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.