Records and Information Management Policy

Section 1 - Audience

(1) This policy applies to all University staff, contractors, volunteers, conjoints, students, work experience placements, 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 and information provide evidence of business activity and are a vital information asset. They drive collaboration and communication, preserve knowledge, provide the foundation to support business activity, support decision making, document rights and entitlements, make up the corporate memory of an organisation, and provide stakeholders with transparency and accountability for University operations.

(3) Having the capacity to securely store records and information in a way that can be readily and efficiently managed, retrieved and re-used is essential to the effective operation of the University.

(4) The University is committed to the principles set out in relevant legislation and whole of government policies. The University has responsibilities for record and information management under the State Records Act 1998 (NSW). This policy is directly aligned with the principles outlined in Standard 12: Standard on Records Management, issued under the State Records Act 1998 and AS ISO 15489.1:2017, Information and Documentation - Records Management.

Section 3 - Purpose

(5) This policy identifies the University's obligations under the State Records Act 1998 (NSW)and the principles of the Standard No 12: Standards on Records Management; and establishes a framework by which the University will govern the management of records and information (including research data).

Section 4 - Policy Scope

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

(7) University records may include, but are not limited to, paper based records, emails, electronic documents, microfilm, tape, photos, camera footage, web pages, social media and structured data held in databases.

(8) This policy does not apply to records and information that only have a limited or incidental relevance to performance of a University function.

(9) This policy does not apply to records and information created and retained at the University of Newcastle Singapore (UONS). UONS records are subject to Singaporean Laws.

Section 5 - Document Specific Definitions

(10) In the context of this document:

a. “high value records” means those University Records that have been identified as supporting high risk or high value business operations including those records which if not controlled would be outside the University’s risk appetite;
b. “Vital Records” means those University Records that have been identified by Information Owners as essential for the ongoing business of the University, without which the University could not continue to function effectively or protect its interests;
c. “University function or activity” means any decisions, actions, risk assessments 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 the health and safety of staff and students, student administration, alumni administration, human resource management, financial management, governance and administration of the University, and commercial activities;
d. “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,(NSW) (commonly referred to as permanent records of the State). Examples of State Archives include, but are not limited to;
    i. master sets of by-laws and 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;
e. “disposal” refers to a range of processes associated with implementing records and information retention, destruction or transfer decisions which are documented in disposal authorities;
f. “University Records Management System” is an approved information system managed by Records Governance Services – TRIM;
g. “University Approved Information Systems” are those systems that are supported by the University and have been assessed by Records Governance Services for suitable record keeping functionality, and Information Technology Services for acceptable security functionality. Refer to Information Security Policy for more information.
h. “data subjects’ under GDPR is anyone within the borders of the European Union (EU) at the time of processing of their personal data.

Section 6 - Principles

University Records and Information Management Program

(11) 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.

(12) The program, including policies, procedures, people and the systems required to manage records and information will be monitored and evaluated so that there is continuous improvements and assurance that the needs of the

University and regulatory requirements are met.

Creation and Management of University Records and Information

(13) Information owners shall assess, document and review those University Records that they are responsible for in accordance with this policy.

(14) Information owners shall ensure that those University Records they are responsible for are created, stored and protected for operational, accountability and compliance purposes within a University Approved Information System.

(15) Information owners shall ensure sensitive, personal and confidential University Records are protected against unauthorised access and are not retained for any period longer than the purpose for which they were collected.

(16) Prior to entering into arrangements to store and manage University Records with third party providers outside of NSW, University Records must be assessed to ensure they can be stored in accordance with the requirements outlined in NSW State Archives and Records GA35 - Transferring Records out of NSW.

(17) Email folders, shared folders, personal drives, or external storage media shall not be used to permanently store University Records as these lack the necessary functionality to protect and manage University Records. University Records held in these systems must be incorporated into the University's Record Management System.

Retention and Disposal of University Records and Information

(18) Retention periods for records and information are set by the State Archives and Records Authority of NSW in the NSW State Archives and Records - Retention and Disposal Authorities. Disposal Authorities are legislated under the State Records Act 1998 (NSW).

(19) Disposal Authorities determine how long records and information need to be kept before they can be disposed. The University uses a number of General and Functional Disposal Authorities to manage retention requirements.

(20) Destruction of University Records prior to completion of minimum retention periods is prohibited under the State Records Act 1998(NSW).

(21) The University has assigned authority for the disposal of records and information in its delegations register.

(22) Disposal of records must be authorised, secure, timely and documented to support compliance with the State Records Act 1998 and Privacy Legislation.

University Records and Information Management Systems

(23) University Approved Information Systems used to capture and manage High Value Records and Vital Records must satisfy the NSW State Archives and Records Standard No 12: Standard on Records Management or be linked to the approved University Records Management System.

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

(25) System Owners 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 and Information

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

(27) Staff are required to comply with the Information Security Policy, Privacy and Information Access Policy and Privacy Management Plan when accessing records and information.

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

Security of University Records and Information

(29) University Approved Information Systems must have appropriate security mechanisms including access and user permissions to protect records and information wherever they are located.

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

(31) Security for physical storage of University Records must be in accordance with Standard 11: Standard on Physical Storage of State Records.

Out-sourcing University Records and Information

(32) Information owners shall ensure that any out-sourced information systems are assessed prior to their use to ensure recordkeeping requirements and risks are managed in accordance with Standard No 12: Standard on Records Management and the University's Risk Management Framework. This will enable the University to meet regulatory and compliance obligations.

State Archives - Transfer of University Records and Information

(33) University Records that are State Archives are required to be transferred to the NSW State Archives and Records Authority when they are at least 25 years old.

(34) Digital State Archives must be migrated to the University’s Records Management System in a suitable long-term format so that they are preserved prior to being transferred to NSW State Archives and Records Authority. This will ensure compliance with the NSW State Archives and Records - Digital Records Preservation Policy.

Migration and Decommissioning of IT Systems

(35) Decommissioning of information systems must be planned and documented, and the plan must take into account retention and disposal requirements in line with the Disposal Authorities.

(36) Records and information migration and conversion processes must be planned, documented and tested to ensure that any University Records that are migrated and or converted remain accurate, reliable, useable and that metadata remains associated with records. This will support the requirements under the NSW State Archives and Records - GA48 Source Records that have been migrated.

Risk and Business Continuity

(37) The University will ensure its Business Continuity Plans for critical processes will identify risks to Vital Records and will provide processes to monitor and manage these risks, in line with the University's Business Continuity

Management Framework.

General Data Protection Regulation – GDPR

(38) Records and information relating to data subjects within the European Union (EU) and relating to University core functions or activities are to be retained in accordance with retention and disposal requirements as per the State Records Act 1998 (NSW). If personal information provided is more than required for University function or activities or relates to marketing activities, then it can be destroyed.

(39) Request to alter records and information should be done so in accordance with the Universities Privacy Management Plan.

Section 7 - Roles and Responsibilities

All staff

(40) All staff are responsible for the management of University Records in University Approved Information Systems in accordance with this policy. Additional responsibilities for certain staff are listed below.

Vice-Chancellor

(41) The Vice-Chancellor is responsible for ensuring the overall management of University Records and information is in compliance with the requirements of the State Records Act 1998 (NSW).

Senior Staff

(42) Senior staff are responsible for the visible support, direction of, and adherence to this policy by promoting a culture of compliant records and information management, and that records and information management programs meet the requirements of the University functions and activities.

Records Governance Services

(43) 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 records and information, and assessment of proposed new information systems.

Chief Information Officer

(44) The Chief Information Officer is responsible for maintaining the technology for the University's business records and 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

(45) 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, and that their staff including contract staff, are aware of and are supported to follow the records and information management principles defined in this policy.

Information Owners

(46) Information owners must ensure that records and information 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

(47) System Owners must ensure that configuration and system design documents that they are responsible for are relevant and up-to-date.

Contract Staff

(48) Contract staff shall create and manage records and information in accordance with this policy to the extent specified in the contract.

Status and Details

Status	Historic
Effective Date	28th September 2020
Review Date	28th September 2021
Approval Authority	Vice-Chancellor
Approval Date	10th August 2020
Expiry Date	28th June 2022
Responsible Executive	Jeanette McElhinney Manager, Records Governance Services
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.

"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.