Records and Information Management Policy

Section 1 - Audience

(1) This policy applies to all University (UON) staff, contractors, conjoint staff, students, work experience placements and members of advisory and governing bodies, in all campuses, locations and controlled entities of the University, to all aspects of the University's business and all business records created and held.

Section 2 - Executive Summary

(2) The University of Newcastle's records and information are a vital corporate asset. The University has responsibilities for record and information management under the State Records Act 1998. This policy is directly aligned with Standard No 12: Standard on Records Management, issued under the State Records Act 1998 and AS ISO 15489.1:2017.

(3) The University is committed to the principles and practices set out in relevant legislation, the whole-of-government policies and relevant standards and to establishing and maintaining records and information management practices that meet business needs, accountability requirements, effective knowledge management, and stakeholder expectations, whilst maintaining security and confidentiality of information, and preservation for future reference.

Section 3 - Purpose

(4) This policy identifies the principles and establishes a framework which will govern the University's management of records and information (including research data). Those principles will ensure that records and information are created, protected and disposed of appropriately and in accordance with statutory requirements.

Section 4 - Policy Scope

(5) This Policy applies to any record and information in any format created, received or maintained by University staff, or anyone performing work on behalf of the University (including contractors and consultants), in the course of carrying out a University function or activity.

(6) State Archives and Records Authority of NSW define a record as any document or source of information compiled, created, sent, received, recorded or stored by any manner or by any other means, in the course of carrying out the business of the University. A record may include, but is not limited to, paper based records, emails, electronic documents, microfilm, tape, spreadsheets, web pages, social media sites, and structured data held in databases. Records are evidence of actions, research and decision making process, show accountability, mitigate risk and protect the University's corporate memory.

Section 5 - Definitions

(7) Disposal means the process by which records or information are either destroyed or retained as permanent State

Archives.

(8) Cloud computing means a model for enabling ubiquitous convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Section 6 - Principles

Establishment of a records and information management program

(9) The University will establish a records and information management program that satisfies the requirements of the State Records Act 1998 (NSW) and any associated standards, policies and guidelines. Creation, implementation and monitoring of this program is the responsibility of Records Governance Services, who reports to the University Secretary and Chief Governance Officer, in collaboration with all business unit managers.

Creation and management of records and information

(10) Full and accurate records of the activities of the University must be created and captured.

(11) Records and information created should provide a reliable and accurate account of decisions and actions, including the names, dates and time, and other key information needed to capture the business context.

(12) All electronic records and information that are created, sent, received, supports business processes and or have archival value, must be stored within UON approved information systems. Approved information systems are those systems that are supported by the University and/or have been assessed by Records Governance Services for recordkeeping functionality.

(13) Records and information must not be maintained in email folders, shared folders, personal drives, or external storage media as these lack the necessary functionality to protect business information over time.

(14) Records and information must not be maintained in cloud applications where the University does not have a contractual agreement with the service provider or where risk and disaster management strategies have not been addressed.

(15) All business information systems used to capture and manage records and information must by design include recordkeeping functionality or be linked to a UON approved information system to support information and records management processes across the University and satisfy the NSW State Archives and Records Standard on Records Management.

(16) Systems being upgraded, including those systems moving into the Cloud must be assessed for compliance against the Standard on Records Management by Records Governance Services prior to the implementation.

(17) Where records and information are stored or processed outside the state of NSW, records must first be assessed to ensure they can be stored outside NSW in accordance with the requirements outlined in NSW State Archives and Records GA35 - Transferring Records out of NSW.

(18) In the event that the management of a University ICT system is outsourced, processes must be carefully developed and documented to ensure that service levels are maintained, and that any residual risks remain within Councils' risk appetite and are managed in accordance with UON's Risk Management Framework.

(19) Outsourcing arrangements must not diminish UON's ability to meet regulatory and/or compliance obligations. Particular attention must be given to sensitive, personal and confidential information and records to ensure they are protected against disclosure to unauthorised individuals.

(20) Information systems must include minimum metadata requirements to support identification, useability, accessibility and context of records and information in accordance with NSW State Archives and the Standard on Records Management.

(21) Appropriate documentation on system design and maintenance must be created to assist with monitoring, auditing and ensuring records and information management systems operate as expected.

Access to Records and Information

(22) Access to records and information is limited to protect:

a. Individual staff and student privacy;
b. Restricted, highly restricted or x-in-confidence material;
c. Legal privilege or ethics in confidence.

(23) Access may be provided (upon approval by the relevant information owner, or staff member with delegated authority) when the records and information are required to complete a legitimate UON function.

(24) Staff are required to comply with Privacy legislation and the Privacy and Information Access Policy and Privacy Management Plan when accessing information.

Security Classifications

(25) Records and information (regardless of format and location) must be classified at the point of creation to inform appropriate security measures for storage and access. Please refer to the Information Security Data Classification and Handling Manual for further details on how to classify records based on sensitivity and potential impact on the University in the event that the information is disclosed, misused, misrepresented or lost.

Retention Periods

(26) Retention periods are set by the State Archives and Records Authority of NSW and take into account all business, legal, audit and government requirements for records and information. The University uses general and university specific disposal authorities to determine retention, destruction and transfer actions for its records and information.

Disposing Records and information

(27) The University is responsible for the safe and secure destruction of records and information (irrespective of where the information is held) when the minimum legal retention requirement has been satisfied. Appropriate, accountable and documented destruction of records and information supports compliance with State Records and Privacy Legislation.

(28) Staff should not destroy any University records and information (including digital records) without the approval of the Records Governance Services.

(29) Information migration and decommissioning of records and information must take into account retention and disposal requirements.

Transfer of records and information

(30) At times, certain records and information may be required to be transferred out of the custody of the University. This occurs when records and information of long term and archival value are no longer being actively used. In these instances, the University transfers those records to NSW State Archives and Records. These records can be readily accessed if a subsequent need arises by contacting the Records Governance Services. Examples include, but is not

limited to:

a. Master sets of by-laws and rules;
b. Master sets of policies;
c. Master sets of Senate, Council and similar governing bodies meeting papers;
d. Annual reports;
e. Registers of Graduates, Scholarships, Ownership of intellectual property, Research project final reports or Student academic transcripts.

Risk and Business Continuity

(31) Risks to records and information must be identified and adequately monitored and managed as per the “Business Continuity Management Framework”. Disaster prevention and response, and recovery strategies for systems containing high risk and high value records and information (also called vital records) must be implemented across the University.

Roles and Responsibilities

(32) All staff are responsible for the creation and management of information and records as set out by this policy. Additional responsibilities for certain staff are listed below.

Vice-Chancellor

(33) The Vice-Chancellor is responsible for the overall management of records and information within the University.

Senior Management

(34) Senior Managers are responsible for the visible support of, and adherence to this policy by promoting a culture of compliant records and information management within the University.

Records Governance Services (RGS)

(35) The RGS is responsible for overseeing the management of records and information at the University consistent with the requirements described in the policy, including the provision of advice, training, authorising the disposal of records and information and approval of new systems used at the University.

Chief Information Officer

(36) 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 audits of systems to ensure that there are no issues affecting information integrity, useability, confidentiality or accessibility.

Managers and Supervisors

(37) Managers and supervisors are responsible for ensuring staff including contract staff, are aware of, and are supported to follow the records and information management practices defined in State Records legislation, and this policy.

Business / System Owners

(38) As part of the development and implementation of new systems business / system owners must ensure that records and information management requirements are identified and managed in accordance with State Record legislation and this policy. Business / system owners are responsible to ensure migration and decommissioning of

systems take into account retention and disposal requirements for records and information held within the system.

Contract Staff

(39) Contract staff should 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	23rd October 2018
Review Date	23rd October 2019
Approval Authority	Vice-Chancellor
Approval Date	15th October 2018
Expiry Date	27th September 2020
Responsible Executive	Jeanette McElhinney Manager, Records Governance Services
Enquiries Contact	

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.

"Term" - When referring to an academic period, term means a period of time aligned to an academic year for the delivery of a course in which students enrol and for which they are usually charged fees for example semesters, trimesters, summer, winter or full-year term. The academic year for a term is determined by the academic year in which the course commences, not concludes. For all other uses of this term, the generic definition applies.