# Records Governance Policy

# Section 1 - Purpose

(1) This Policy:

a. establishes how the University of Newcastle (University) meets its obligations under the State Records Act 1998 (NSW), State Records Regulations (2015), and the State Records NSW Standard on Records Management;
b. outlines how the University governs the management of University records including minimisation of risks relating to University records; and
c. determines how the University will preserve University records that are of corporate and community significance.

# Section 2 - Scope

(2) This Policy applies to all University records. University records are records, as defined by the State Records Act 1998 (NSW), that:

a. may be in any physical or digital format, including but not limited to:
    i. paper based records;
    ii. databases;
    iii. emails;
    iv. scanned documents;
    v. records created in collaboration sites such as (but no limited to) MS365 – Teams, Sharepiont, OneDrive;
    vi. records created in cloud-based third party applications;
    vii. microfilm;
    viii. tape;
    ix. photos;
    x. video footage;
    xi. webpages;
    xii. social media content;
    xiii. maps; and
    xiv. research data.
b. are created, received or maintained by the University; and
c. documents any University function or activity, including:
    i. a decision (in the positive or negative);
    ii. a binding commitment;
    iii. research;
    iv. deliberation, advice, evidence, or actions.

(3) This Policy does not apply to University records that are:

a. classified as State archives and are under the control of Museums of History NSW in an approved State archives facility. Some of the University's physical State archives are managed in in the University's Special Collections unit. (These records are bound by the Art and Special Collections Management Framework); or
b. created and retained at the Newcastle Australia Institute of Higher Education (Singapore) campus and are not subject to the State Records Act 1998, unless stipulated in an agreement or constitution.

# Section 3 - Audience

(4) This Policy should be read and understood by all University staff, contractors, volunteers, students, work experience participants, members of advisory and governing bodies, and staff of controlled entities of the University ("personnel").

# Section 4 - Definitions

(5) In the context of this Policy:

a. "Access Directions" refers to the State Records NSW framework for regulating public access to State records. Any State record which has been in existence for more than 20 years will be open to public access by default, unless a 'closed to public access (CPA) direction has been made. Records can also be subject to an 'early access (EA) direction', which will open them to public access after a shorter period of time;
b. "appraised" or "appraisal" refers to the recurrent process of evaluating business activities to determine which records need to be created and captured as well as how and how long the records need to be kept. It combines an understanding of business activities and their context with:
    i. the identification of business needs, regulatory requirements and societal expectations relating to records; and
    ii. the assessment of opportunities and risks associated with the creation and management of records;
c. "data subjects" under the General Data Protection Regulation (GDPR) includes any person within the borders of the European Union (EU) at the time of processing of their personal information;
d. "destruction" or "destroy" means the complete and irreversible physical erasure of a University record(s) which ensures that it cannot reconstituted or reconstructed;
e. "Digital Technology Solutions Approved Information System" means an information system supported by the University, which has been assessed by Digital Technology Solutions for acceptable security functionality (refer to Information Security Policy ). These systems are not compliant with the requirements of this Policy;
f. "disposal" means the range of processes associated with implementing appraisal decisions. These include the retention, deletion or destruction of University records in or from a recordkeeping system. This may also include the migration of University records between recordkeeping systems, and the transfer of custody or ownership of University records (State Records Act 1998);
g. "Head of Organisational Unit" means the most senior staff member of the University within an individual organisation unit who is responsible for the operation and activities of the relevant unit. A unit is a distinct organisational unit included in the University organisation structure (see Organisation Chart);
h. "high risk records" means those University records that are created in high risk business processes or functions, or received in high risk areas of the University, and that are considered at a level of risk that is outside the University's risk appetite should they be misused, released inappropriately, inappropriately accessed and altered, lost, damaged, or destroyed prematurely;
i. "high value records" means those University records that enable the University to continue their functions, provide a service, and respond to Royal Commissions, inquiries, audits, investigations and legal issues;
j. "inactive University records" refers to University records that are no longer required to meet immediate

business needs, but which must be kept (in accordance with retention and disposal authorities) to support business activities, legal or regulatory requirements, or community expectations;

k. "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 ongoing business or accountability purposes. Examples include:
    i. working papers that are primarily facilitative where 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 that 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 are not required for ongoing business purposes;
    v. published or reference material; and
    vi. personal communications not relating to University functions or activities;

l. "personnel" refers to all persons and parties mentioned in Clause 4 of this Policy;

m. "records management" refers to the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records;

n. "retention period" refers to the minimum period of time for which records should be kept to meet regulatory, business, and community requirements before they can be destroyed;

o. "sensitive information" is as defined by the Privacy Act 1988 (Commonwealth);

p. "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 Museums of History NSW 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;

q. "University Approved Information System" is an information system supported by the University which has been assessed and endorsed by both Records Governance Services as having suitable recordkeeping functionality (either natively, or by taking action to address recordkeeping gaps); and Digital Technology Solutions for acceptable security functionality (refer to Information Security Policy). A register of University Approved Information Systems is available on the Records Governance Services website;

r. "University function or activity" means any decision or action undertaken by or on behalf of the University to further its statutory objectives, including but not limited to:
    i. research;
    ii. research administration;
    iii. teaching, strategic and business planning;
    iv. ensuring health and safety;
    v. student administration;
    vi. alumni administration;

vii. human resource management;
viii. financial management;
ix. governance and administration of the University; and
x. commercial activities;

s. “University records” refers to records that meet the requirements of clause 2 of this Policy;
t. “University Records Management System” is the primary recordkeeping system for the University. This system (Content Manager – TRIM) is managed by Records Governance Services, and has the capability to compliantly manage records.

# Section 5 - Context

(6) University records provide evidence of teaching, research and administration and are a critical asset that is essential to the efficient and effective operation of the University.

(7) The State Records Act 1998 (NSW) establishes record management obligations on the University, including but not limited to:

a. creating and maintaining full and accurate records of all University activities;
b. establishing and maintaining a records management program; and
c. reporting on the implementation of the records management program to State Records NSW.

(8) The University may be obligated under international, State or Commonwealth legislation to maintain, reproduce, or retrieve records.

### University Records Management Program

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

(10) The program, including policies, procedures, people, and systems required to manage University records, will be regularly monitored and evaluated to give assurance that the needs of the University, community and the regulatory requirements are met.

### Ownership, control and custody of University Records

(11) All University records created or received while performing a University function or activity are the property of the University, unless otherwise specified under contract, and must be managed in accordance with this Policy.

# Section 6 - Record Creation

(12) University records must be created in a way that ensures the record is reliable, accurate, usable, stored and appropriately protected within the University Records Management System (Content Manager – TRIM) or a University Approved Information System. Physical records may be stored and protected in a storage area that is assessed by Records Governance Services as compliant. (Please see State Records NSW Records Systems Characteristics and Functions).

(13) Sensitive information, personal information, and confidential information that constitute University records must:

a. be protected against unauthorised access;
b. not be kept for any longer than necessary; and

c. be destroyed in accordance with this Policy.

# Section 7 - Retention

(14) Retention periods for University records are set by 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.

### Appraisal of Records

(15) Records Governance Services ensures that the configuration and implementation of Content Manager – TRIM is such that University records are appraised when the record is created in or transferred to Content Manager – TRIM. All University records are required to be appraised, or re-appraised, before being disposed of or destroyed.

### Inactive University Records

(16) Inactive physical University records can be moved to approved storage repositories in consultation with Records Governance Services.

### General Data Protection Regulation – GDPR

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

# Section 8 - Protection of University Records

(18) University records must be subject to protection and preservation, in accordance with the State Records Act, or any other relevant legislative instrument.

(19) Unless in accordance with normal administrative practice, or required under the State Records Act or any other relevant legislative instrument, University records must not be:

a. abandoned;
b. disposed of, unless in accordance with this Policy;
c. transferred, offered to be transferred, or arranged to be transferred, in terms of possession or ownership;
d. taken or sent outside of New South Wales;
e. damaged or altered; or
f. neglected in a way that causes or is likely to cause damage to the University record.

# Section 9 - Disposal or destruction of University records

(20) Personnel are strictly prohibited from destroying University records prior to the completion of the minimum retention period. Penalties exist under the State Records Act 1998 (NSW) for early unauthorised destruction. University records that have limited or incidental relevance can be destroyed in accordance with Normal Administrative Practice (NAP). Schedule 2 of the State Records Regulation 2015 provides guidelines on what constitutes Normal Administrative Practice.

(21) Destruction of University records must be:

a. authorised in accordance with the University's delegations of authority (see Delegations Register), subject to endorsement from Records Governance Services using the Record Destruction Authorisation Form; and
b. undertaken in a secure, timely and documented manner to minimise risks associated with records being accessible beyond their requirements.

(22) Following approval, the destruction of University records must be in accordance with the State Records NSW - Destruction of Records Guideline. The completed Record Destruction Authorisation Form must include:

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

(23) Evidence of destruction must be obtained and provided to Records Governance Services.

(24) Physical University records may be destroyed prior to their minimum retention requirements where the following is complied with:

a. the records must be digitised prior to their destruction in accordance with State Records NSW – General Retention and Disposal Authority GA45 – Original or source records that have been copied (GA45);
b. the records must be stored in Content Manager – TRIM or a University Approved Information System; and
c. if required, a Records Digitisation Project Plan and Record Destruction Form for Digitised Original or Source Records must be completed by the Head of the Organisational Unit or their nominee, and authorised by Records Governance Services. This is a requirement for digitisation projects, and for an ongoing digitisation activity for a group of records.

(25) Clause 24 do not apply to the following records. These are excluded from the provisions of GA45 and cannot be destroyed after being digitised:

a. records that are required as State archives that were created prior to 1980; and
b. film, photograph negatives, or analogue audio-visual material that are required as State archives.

### State Archives – Transfer of University Records

(26) Physical and digital records that are identified as “State archives’ and that are no longer needed by the University for ongoing business must be transferred to an approved Museums of History NSW archives facility. This must be undertaken by Records Governance Services.

(27) Records Governance Services are responsible for developing and submitting a plan to Museums of History NSW outlining the University's intention to transfer records that are required as State archives. Transfer Plans are required to be submitted every five years, and the requirement to submit a Transfer Plan applies even if there is no intention to transfer records.

# Section 10 - Access to University Records

### Access Management

(28) Heads of Organisational Units 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 information, personal information, health

information, and confidential records. Access must be monitored to ensure all access remains relevant and current, and a person's access must be removed once it is no longer required.

### Compliant Access

(29) All personnel must comply with the:

a. Information Security Policy, Privacy Policy and Privacy Management Plan and their associated documents when accessing University records; and
b. Research Data and Primary Materials Management Procedure when accessing research data / primary material.

(30) Access to University records that are not made publicly available by the University may be provided to external parties if:

a. considered permissible under all relevant University policies, or where required by law. (Please also refer to the Agency Information Guide); and
b. where required, authorised by a relevant delegate; or
c. where not required to be authorised by a relevant delegate, authorised by the Head of the Organisational Unit.

### Obligation to maintain accessibility to equipment / technology dependent records

(31) If a record is in such a form that information can only be produced or made available from it by means of the use of particular equipment or information technology (such as computer software), the Head of the Organisational Unit must take such action as may be necessary to ensure that the information remains able to be produced or made available.

### Access Directions

(32) The State Records Act 1998 (NSW) promotes the principle of open government by presuming all records are open to public access by default after 20 years.

(33) Heads of Organisationa Units are responsible for identifying University records they are responsible for, and that are older than 20 years, that require 'Closed to Public (CPA) directions' or 'early access (EA) directions'. Records Governance Services are responsible for submitting required access directions as per Museums of History NSW – Public Access to State Records Guidelines.

(34) CPA directions will expire after 5 years and must be actively renewed. If they are not renewed, the records covered by the expired access direction will revert to being open once they are more than 20 years old. Records Governance Services are responsible for monitoring and renewing expired access directions.

# Section 11 - University Approved Information Systems

(35) University Approved Information Systems must include minimum metadata requirements to support identification, usability, accessibility and context of University records in accordance with State Records NSW Standard on Records Management.

(36) Information systems that capture and store high value records and high risk records must comply with the requirements of the State Records NSW Standard on Records Management, or be integrated with Content Manager - TRIM.

(37) Heads of Organisational Units must consult with Records Governance Services prior to implementing new information systems, or upgrading existing University Approved Information Systems to ensure record management requirements and obligations can be met.

(38) 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 systems operate as expected.

### Out-sourced Information Systems

(39) Heads of Organisational Units must assess out-sourced information systems prior to their use to ensure:

a. recordkeeping requirements meet the State Records NSW Standard on Records Management; and
b. risk management is in accordance with the University's Risk Management Framework.

### Decommissioning and Migration of IT Systems and Data

(40) Decommissioning of University Approved Information Systems or Digital Technology Solutions Approved Information Systems and associated 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.

(41) 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).

# Section 12 - Records Management Program

### Risk and Business Continuity

(42) Heads of Organisational Units 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.

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

(44) The University will ensure its business continuity plans for critical processes identify 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.

### Personnel / Organisational Change

(45) Heads of Organisational Units 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:

a. leaving the University,
b. moving divisions, business units, or premises; or
c. when there is a restructure.

### Monitoring of Record Management

(46) Records Governance Services are responsible for the regular assessment of the effectiveness and efficiencies of recordkeeping processes 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. assessing compliance against the State Records Act 1998;
b. benchmarking against State Records NSW Standard on Records Management using the Records Management Assessment Tool (RMAT);
c. assessment against plans, goals and objectives of the business unit records management program, in consultation with the Head of Organisational Unit;
d. review of recordkeeping and record management practices;
e. conducting detailed reviews of high risk business areas to confirm that records are being created and captured into the recordkeeping system; and
f. assessing records management system and business systems that create and capture records.

# Section 13 - Roles and Responsibilities

### Personnel

(47) All personnel are responsible for the creation and management of University records in accordance with this Policy.

(48) All new staff to the University:

a. must complete the Integrity Module within Discover which details the recordkeeping requirements for the University; and
b. may request access to Content Manager – TRIM via ServiceNOW.

### Vice-Chancellor

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

### Heads of Organisational Units

(50) Heads of Organisational Units are responsible for ensuring adherence to this Policy by supporting and implementing comprehensive records management programs and promoting a culture of compliant record management that meets the requirements of the University and its stakeholders.

(51) Heads of Organisational Units must:

a. ensure that record management requirements are identified and managed in accordance with this Policy;
b. apply the Records and Information Risk Assessment Guide to determine the best way to manage and store records;
c. ensure that the development and implementation of any new University Approved Information Systems or Digital Technology Solutions Approved Information Systems that they are responsible for is managed in accordance with this Policy;
d. consult with Records Governance Services regarding compliance of new or existing information management systems;

e. 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;
f. apply Access Directions, where relevant, and in accordance with this Policy; and
g. assess any out-sourced information management systems prior to their use.

## University Secretary

(52) The University Secretary is the Senior Responsible Officer, as required by State Records NSW, and has oversight of records management at the University.

## Records Governance Services

(53) Records Governance Services is responsible for:

a. overseeing the management of the University records management program, consistent with the requirements described in this Policy;
b. the provision of advice and training in relation to record management;
c. approving the disposal or destruction of University records;
d. assessing proposed new and existing information management systems for suitable recordkeeping functionality;
e. control and administration of Content Manager - TRIM;
f. being the single point of contact for the University off-site record storage contractor; and
g. administering Access Directions.

## Chief Digital & Information Officer

(54) The Chief Digital & Information Officer, or their nominee, 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

(55) 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 management is integrated into work processes and systems, and that their staff (including contract staff), are aware of and are supported to comply with the requirements of this Policy.

## System Owners and System Administrators

(56) System Owners and System Administrators must ensure that the systems they are responsible for meet the requirements of this Policy and State Records NSW Standard on Records Management and configuration and system design documents are relevant and up-to-date.

## Contract Owners of Managed Service Providers

(57) 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.

# Section 14 - Schedules and Appendices

(58) Record Destruction Authorisation Form;

(59) Records Digitisation Project Plan;

(60) Record Destruction Authorisation Form for Digitised Original or Source Records;

(61) Records and Information Risk Assessment Guide;

(62) General Retention and Disposal Authority: Higher and Further Education(GA47);

(63) General Retention and Disposal Authority: Administrative Records (GA28);

(64) General Retention and Disposal Authority: Public Health Services Patient Records (GDA17);

(65) FA402 Cultural, Recreational and Sport Institutions ;

(66) FA404 Childcare Services.

## Status and Details

| | |
|---|---|
| **Status** | Historic |
| **Effective Date** | 29th November 2023 |
| **Review Date** | 29th November 2025 |
| **Approval Authority** | Vice-Chancellor |
| **Approval Date** | 27th November 2023 |
| **Expiry Date** | 16th September 2024 |
| **Responsible Executive** | Hamish Lithgow<br>University Secretary |
| **Enquiries Contact** | Nerida Lithgow<br>Manager, Records Governance Services<br><br>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-ordinated activities of assessing, controlling, monitoring, and reviewing risk in the pursuit of the University's objectives.

**"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.

**"Confidential information"** - All information which is disclosed to a party by, or on behalf of, the other party, or which is otherwise acquired by a party from the other party, or any adviser engaged by the other party, which: (a) is by its nature confidential; (b) is designated by the other party as being confidential; or (c) the party knows or ought to know is confidential, but does not include information which: (d) is or becomes public knowledge other than through a breach of confidentiality; (e) was already in the possession of a party and not subject to an obligation of confidentiality; (f) is lawfully received from a third party; or (g) is independently developed by a party.

**"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.

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

**"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.

**"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.