Records Management Procedure

Section 1 - Purpose

(1) This procedure supports the Records Management Policy by setting out processes and requirements to ensure the safe custody and proper preservation of University records.

Section 2 - Policy

(2) See the Records Management Policy.

Section 3 - Procedures

Part A - Identify and create records

Identify record needs

(3) Organisational units will determine the University records they need to create and keep by considering:

a. applicable legal obligations and other external drivers relevant to their function, including legislation, regulatory requirements, mandated standards and contract obligations
b. evidence required when an authority is exercised and other requirements under rules, delegations and policies relevant to their function
c. business requirements of the unit
d. internal and external expectations for evidence, information, accountability and scrutiny
e. relevant NSW general disposal authorities
f. advice from the University's Policy and Records unit.

(4) The following resources may help an organisational unit identify its record needs:

a. Common records and tips for identifying record requirements [link to be added]
b. Record and information asset management plan template
c. Records management guide - managing web content

Create records

(5) University records must be routinely created during the normal business practice of individuals, organisational units and committees, to provide evidence of decisions and actions taken as part of their work or function.

(6) If an activity does not automatically generate records (e.g. business activities or transactions performed in an information system), processes must be established to create them (e.g. minutes taken at meetings, recording a conversation or documenting it afterwards).

(7) University records must be reliable and trustworthy with enough information and metadata to give meaning and

context to the record. This might include capturing additional information about who made a decision, when, why or under what authority, if a system based process does not automatically capture this.

Part B - Store, use and protect records

Record storage requirements

(8) University records must be stored in an appropriate system or location that allows them to be:

a. identifiable, retrievable and accessible for as long as they are required
b. protected from unauthorised or unlawful access, destruction, loss, deletion or alteration.

(9) In addition to the provisions in this part, some record types will have specific requirements under other University policies or procedures, including but not limited to:

a. Research Data Management Procedure
b. Legal Procedure - Legal Records

(10) University records (both physical and electronic/digital) that are stored outside of New South Wales must be done so in accordance with the general disposal authority GA35 – Transferring records out of NSW [etc].

High risk and high value records

(11) The Records Management Policy provides the criteria for identifying high risk and high value records. All high risk and high value records and information must:

a. be registered on the information asset register (maintained by the Office of Governance and Corporate Administration) with details about where/how they are stored and how the records management compliance obligations are being met
b. be included in business continuity plans for critical processes, identifying risks to the records and processes for monitoring and managing those risks.

Electronic records and information systems

(12) Electronic/digital records must be captured as soon as practicable in a University-managed information system, such as one of the following:

a. The system of record: the business information system that creates the record, with appropriate controls and processes in place to ensure compliance obligations are met (e.g. Banner, Interact2, Ascender, CASIMS/CDAP, Tweek!, Protecht or CRM).
b. A records management system: one of the University's approved, compliant record-keeping systems (e.g. Unirecords for corporate records, Banner Document Management for student records).
c. A general purpose data storage system: for records that are not high risk or high value, University supported storage or platforms (e.g. shared/S drive, Confluence or OneDrive) may be used, with appropriate controls and processes in place to ensure compliance obligations are met.

(13) Exchange Online (the University email system) will retain captured emails for seven years (for non-executive staff) or permanently (for executive staff). However, Exchange Online is not a records management system and appropriate controls and processes must be used to meet compliance obligations such as longer retention periods, privacy, security, and disposal. These requirements must be determined based on the content of the email and the activity or transaction it records.

(14) Microsoft Teams is a communication and collaboration tool, which does not have the necessary functionality and controls to be an appropriate recordkeeping system. Therefore, staff must ensure that their communications are documented appropriately.

(15) Organisational units can assess whether an information system meets their recordkeeping compliance obligations using the NSW State Archives and Records checklist for assessing business systems. The checklist also details whether additional controls or processes are required for a record or system. The Policy and Records Unit can be contacted for assistance.

(16) Information systems must be reassessed for records management compliance if they undergo major upgrades or changes in functionality or content. This includes instances where systems move from the University to an external service provider.

Physical records

(17) Digitising records is preferred to physical storage, except where:

a. the time and resources required would not be proportionate with the value or retention requirements of the records in scope
b. digitisation is not appropriate for the existing format of the record
c. destruction of the original or source record would not be allowed under general disposal authority GA45 – Original or source records that have been copied.

(18) Physical records must be stored in suitable locations and protected from loss, damage or unauthorised access in accordance with the NSW standard on the physical storage of State records.

(19) Where physical records are digitised:

a. the physical record must be retained for at least three months to allow for quality assurance or disaster recovery. After this, a request to destroy should be made in accordance with this procedure
b. the digitised records must be in a sustainable file format, in line with the State Archives and Records Authority's preferred file formats and specifications.

Records that must be stored in Unirecords

(20) Certain University records must be captured into the University's corporate records management system, Unirecords:

a. Unirecords provides the University's contract register. Signed agreements, contracts, leases and licenses must be captured in Unirecords as soon as possible. Where the value of the agreement etc. exceeds $150,000, it must be registered and captured in Unirecords within 40 days of signing, to enable reporting and disclosure as required by the Government Information (Public Access) Act 2009 (GIPA Act).
b. Electronic records with a permanent retention period (that is, required as State archives) must be stored in Unirecords. Exemptions are permitted where the record is comprised of structured data and metadata elements in a system of record, or as otherwise authorised by the Manager, Charles Sturt University Regional Archives & University Art Collection.

(21) More information about Unirecords is available on the Records Management website.

Security of records

(22) All University data, information and records must be classified under the University's Information Classification

and Handling Procedure as either:

a. public
b. internal
c. confidential, private
d. highly confidential.

(23) To promote efficient business practices, University records should by default be classified as 'internal' unless:

a. there is a reasonable need to make the records 'confidential, private' or 'highly confidential' (eg. personal or health records, commercial in confidence records)
b. the records can be classified as 'public' because they are intended for public disclosure and consumption, or are otherwise identified as the University's open documents under the GIPA Act.

(24) Access, security and user permissions for University systems and locations holding University records and information must be documented and implemented.

(25) Security requirements for University systems are set out in the Information Technology Policy and the Information Security Guidelines.

(26) Security for physical storage of University records must be in accordance with the Standard on Physical Storage of State Records – Principle 6.

(27) The Division of Information Technology document storage matrix includes information about the security capabilities of University information systems.

Access to records

(28) See the Records Management Procedure – Access.

a. Note: this procedure is in development and will consolidate:
    i. Records Management Procedure - Access to University Records
    ii. Personal Files Access Policy
    iii. Records Management Policy - Student Records and Assessment Items Access

Part C - Retention and disposal of records

Retention

(29) Minimum record retention periods for NSW public offices are set through general retention and disposal authorities (GDA) under the State Records Act. The Archiving and destroying records website lists GDAs that apply to University records.

(30) Minimum retention requirements may also be specified in other legislation, standards or University policies applicable to a business activity. Where different retention periods apply, the longer one must be satisfied.

(31) Notwithstanding clauses 28-29, a direction from any court or tribunal, statutory body, commission or governing agency, must also be satisfied.

(32) University records may be kept for longer than the minimum retention period if they are required for ongoing business purposes, or for historical or research purposes. Longer retention requires consideration of the University's business needs, resource impacts, public interest and privacy obligations.

(33) Where University records held beyond the minimum retention period contain personal, sensitive or health information (as described in the Privacy Management Plan) the new retention period should be discussed with the University Ombudsman (as the University's privacy officer).

State and University archives

(34) University records identified as State archives (requiring permanent retention) or requiring long term retention (50+ years) must be transferred to the CSU Regional Archives or captured in Unirecords once administrative use ceases.

(35) Access directions must be in place for all University records that are 30+ years old. The University has a number of access directions approved by the State Archives and Records Authority.

Destruction of records

(36) University records (including records held in information systems or with service providers) must only be destroyed where either:

a. the destruction has been approved via an application for destruction (see the 'Requests to destroy' heading below)
b. a pre-approval for the destruction has been authorised (see the 'Pre-approval to destroy' heading below)
c. the disposal or destruction is allowed under normal administrative practice (NAP) (see the 'Normal administrative practice' heading below).

(37) University records may only be destroyed where there are no disposal alerts, court orders or other disposal suspension directives in place related to the records.

(38) The destruction of University records must be undertaken in a secure manner that is appropriate to the format and relevant security classification.

(39) Destruction of University records must be documented (unless destroyed under NAP) with a record of destruction retained in accordance with the relevant retention and disposal authorities.

(40) Information about appropriate methods of destruction of records is available from NSW State Archives and Records.

(41) UniMarket lists the document shredding and recycling companies that may be used for the destruction of University paper records.

Requests to destroy

(42) Organisational units wishing to destroy University records must complete an Authority to destroy records form. This form must be signed by:

a. the Manager, Policy and Records, to confirm that retention requirements have been met
b. the appropriate unit manager, to confirm the records are no longer required for business purposes
c. the party undertaking the destruction, to confirm that the records have been securely destroyed. This may be an external party (e.g. the system vendor for decommissioned systems or a document shredding/recycling company).

(43) The completed, signed authority must be returned to the Manager, Policy and Records for capture and retention in Unirecords.

Pre-approval to destroy

(44) Pre-approval to destroy University records may be given where:

a. the record is not high risk or high value
b. the minimum retention period is low (generally less than two years or 'until administrative reference use ceases')
c. using an information system's automated deletion functions would better meet the University's obligations for the secure, confidential and timely destruction of personal or sensitive information than submitting a request to destroy.

(45) Pre-approved destruction processes must:

a. be authorised by the Manager, Policy and Records and the appropriate unit manager
b. have a means of documenting the destruction (e.g. an audit log) that can be retained in accordance with the relevant retention and disposal authority
c. be regularly monitored and reviewed by the organisational unit.

Normal administrative practice

(46) The State Records Regulation allows certain records to be disposed of as part of normal administrative practice (NAP) with no further approval or documentation required.

(47) The following are types of University records that may be destroyed under NAP, however, see schedule 2 of the State Records Regulation for exceptions:

a. drafts and working papers (e.g. background notes, reference materials) that do not contain significant decisions, discussions or rationale not covered by the final record
b. copies or duplicates of University records
c. computer support records once they have been acted upon or superseded and are not required for ongoing business requirements
d. ephemeral facilitating instructions
e. low risk, 'for your information' messages that do not require action by the recipient
f. unused forms, stationery and templates
g. externally published material including solicited and unsolicited advertising material.

(48) The destruction of University records under NAP must be undertaken in a secure manner that is appropriate to the format and content of the record.

Part D - Miscellaneous

Monitoring the records program

(49) Records and information management activities, systems and processes must be monitored for accountability and to ensure business needs are being met.

(50) The Manager, Policy and Records will conduct reviews and report on overall compliance with the State Records Act and the Records Management Policy as required under the Compliance Management Procedure.

(51) Organisational units must ensure that their high risk, high value information assets are accounted for in their business continuity plans under the Resilience Policy.

(52) Security and access to information systems holding University records must be monitored and reviewed in accordance with the Information Security Guidelines Part D.

Employees leaving their position

(53) When an employee leaves their position they must make arrangements for the ongoing custody of University records for which they were responsible. This includes ensuring records are left accessible to others or ensuring records that are no longer required have been properly stored or destroyed in accordance with this procedure.

Section 4 - Guidelines

(54) Nil.

Section 5 - Glossary

(55) This procedure uses terms defined in the Records Management Policy, as well as the following:

a. Access direction – means a direction that a series, group or class of records is open to public access after 30 years or closed to public access for a longer period of time to protect sensitive information.
b. Administrative use – means records that are still in use by the organisational unit and/or for the business purpose for which it was created. Under the State Records Act, records more than 25 years old are presumed not in use.
c. Digitising – means converting a physical record to a digital format for management and preservation (e.g. scanning or imaging a physical document, transferring tape or disc recordings to computer storage).
d. Normal administrative practice – means the process allowing for the lawful disposal of low value, transitory or ephemeral records generated or accumulated as part of standard business practices, as outlined in Schedule 2 of the NSW State Records Regulation 2015.

Status and Details

Status	Current
Effective Date	18th July 2024
Review Date	29th March 2025
Approval Authority	University Secretary
Approval Date	18th July 2024
Expiry Date	Not Applicable
Unit Head	Anthony Heywood University Secretary
Author	Vanessa Salway Manager, Policy and Records
Enquiries Contact	Policy and Records