Recordkeeping Standard

Version	Approved by	Approval date	Effective date	Next full review
2.0	Director of Governance	13 December 2021	13 December 2021	December 2024

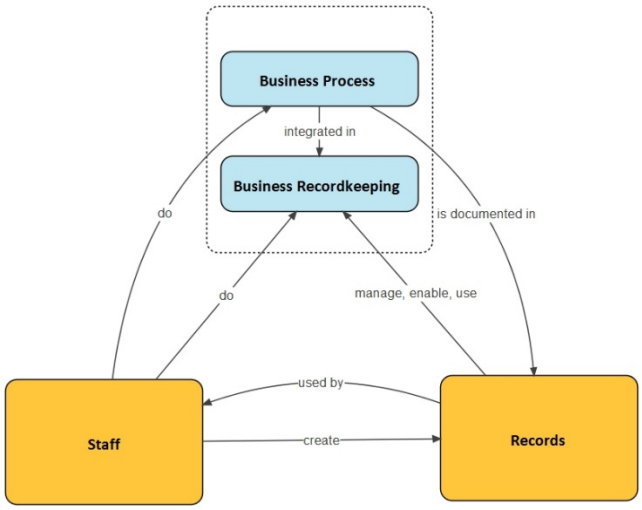
Standard Statement		
Purpose	The University's records are its corporate memory, provide evidence of actions and decisions and represent a vital asset to support its daily functions and operations. This Standard details the requirements of the *Recordkeeping Policy* and specifies the recordkeeping procedures and responsibilities to meet these requirements.	
Scope	All staff, contractors and consultants engaged in work for the University across all of its sites.	
Are Local Documents on this subject permitted?	☐ Yes, however Local Documents must be consistent with this University-wide Document	☒ No
Standard		

1. University Records

A University record is any document, regardless of format, created or received by University staff in the course of their official duties and kept as evidence of the transaction of business activities.

Records provide evidence of what was said and done, where, when, and by whom in the conduct of University work.

Records have a lifecycle that begins with the action which informed their creation, continues with their capture to an official business system and subsequent management over time until they become inactive, and continues through to the process of disposition where they may be destroyed if no longer required or receive new meaning as they are arranged with other records as archives of the University and/or State of NSW and retained permanently.



2. Record Capture and Format

The capture of a record as near as possible to the point of its creation and in its original format saves resources, increases evidentiary value and aligns recordkeeping to better business outcomes.

In contrast, a record captured at the end, not start, of its lifecycle represents an additional step requiring additional resources with reduced added value to business process.

Recordkeeping should be an inherent, integrated and allocated part of everyday business.

3. UNSW Recordkeeping Introduction

All new staff of the University must complete the Introduction to Recordkeeping at UNSW. This is an online module that details the requirements for recordkeeping at the University.

The module allows the University to ensure all staff are aware of the University's commitment to best practice recordkeeping and provides staff with access to all necessary resources to achieve this. To locate the module, please refer to the UNSW Records & Archives website.

All staff have an obligation to be aware of their responsibilities to make and keep full and accurate records of their activities, and how to meet these responsibilities.

Further training and resources on all aspects of University recordkeeping are available at the UNSW Records & Archives website.

4. Systems of Record

A record must be created and captured to a University System of Record. These are business systems that have been evaluated to ensure the requirements of a record are met, such as their evidentiary fixed nature, retrievability, security controls, and disposal management. A UNSW System of Record must be:

- a system that is managing UNSW records
- capable of meeting any specific legislative requirements for these records
- able to capture (and return) fixed, complete, authentic, reliable, useable records
- able to capture (and show) core metadata (description, structure, context, related, events, retrieval information) now (and beyond the life of the record itself.)
- secure and able to restrict access to records (and metadata) (or groups of records) to meet accountability, legislative and business requirements
- able to prevent deletion of records and metadata unless as part of authorised disposal activity
- able to capture an audit log of system activity
- able to support migration and/or controlled disposal of records depending on the period of time for which records must be retained.
- authorised as a UNSW system of record, have an identified system owner and business owner and have its status as a system of record reviewed in line with the requirements of the Record Classification (see section 5).

4.1. Records and Archives Management System (RAMS)

The University provides access to its EDRMS (Electronic Document and Records Management System) known as RAMS (Records and Archives Management System) for all staff.

RAMS is an enterprise recordkeeping system accessible to all University staff for the secure capture of business records not directly captured by alternative systems of record.

RAMS is a system of record with extensive security controls in accordance with the Record Classification (see section 5). For managing record security in RAMS, please refer to the RAMS Information Security guidance.

4.2. Assessment process

The assessment process for Systems of Record is based on the NSW State Archives & Records Authority, Business Systems Assessment Checklist for Recordkeeping, the NSW *Standard on records management*, ISO 16175 *Principles and Functional Requirements for Records in Electronic Office Environments* and the National Archives of Australia, Business System Assessment Framework.

The assessment is to be completed by the System Owner and is maintained by the Records & Archives unit.

Further information and resources can be located on the Records & Archives website.

4.3. Record Security Classification and Review

Those systems evaluated for the capture of University records and information provide for the secure storage of records in accordance with the Record Classifications.

For those systems managing records classified as Highly Sensitive, Sensitive and Private, the information security controls must be reviewed every 6, 12 or 24 months, respectively.

Record Classification	Security review period
Highly Sensitive	6 months
Sensitive	12 months
Private	24 months

Table 1: Record classification review periods

5. Record Classification

Records are classified based on the requirements of the UNSW *Data Classification Standard* for the assessment of records and information based on the adverse impact a breach of this information would have on the University.

All records captured to a University System of Record acquire a fundamental level of security applied to all the University's business systems. Only University staff may log into the system using their staff credentials, and audit logs are generated to monitor system usage and ensure all activity is in line with business need.

This basic level of record security is known as *Private* and applies at a minimum to all records and information managed by University Systems of Record.

All records at the University must have an appropriate security classification applied. This is the responsibility of business owners.

5.1. Classifications

For further information on, and examples of, these classifications please refer to the UNSW *Data Classification Standard*.

Highly Sensitive

Information that if breached owing to accidental or malicious activity would have a high impact on the University's activities and objectives.

Sensitive

Information that if breached owing to accidental or malicious activity would have a medium impact on the University's activities and objectives.

Private

Information that if breached owing to accidental or malicious activity would have a low impact on the University's activities and objectives.

Unclassified

Information that if breached owing to accidental or malicious activity would have an insignificant impact on the University's activities and objectives.

6. Security

A record contained in any business system requires appropriate security controls to ensure that:

- the University's information is secure but still accessible to those who require access for business purposes.

- we meet our commitments to the Information Protection Principles as set out in the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act), the University's *Privacy Policy*, Student Privacy Statement, and the Human Resources Privacy Statement.

All records at the University must have an appropriate security classification applied, this is the responsibility of business owners.

System owners have an obligation both to be aware of the record security classification of the records and information managed by the system and, to ensure the system's compliance with the requirements for this security classification.

Please refer to section 5, Record Classification and section 3, System of Record (section 4) for further information.

7. Storage

Records must, irrespective of format, be stored in an appropriate, secure location.

The University maintains an enterprise recordkeeping system, RAMS, and Systems of Record for the secure capture and management of records.

Please refer to the Systems of Record Guideline for further information.

The University has a preferred supplier for the storage of physical records that provides compliant storage conditions, and the ability to retrieve, scan, and to destroy records when it is appropriate to do so.

Please refer to Appraisal (see section 9) for further detail.

8. Personal Information

Personal information is defined in the NSW *Privacy and Personal Information Protection Act 1998* (PPIP Act) as, 'Information or an opinion (including information or an opinion forming part of a database and whether or not in a recorded form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'.

Personal information should always be destroyed when it is no longer required for the business purpose for which it was collected and there is no legal requirement to retain it further. It must be stored securely at all times and disposed of appropriately as required by both the Information Protection Principles of the PPIP Act and the Health Protection Principles of the NSW *Health Records and Information Privacy Act 2002* (HRIP) Act.

Refer to the *Privacy Policy* and the Compliance Unit website for further information on the requirements relating to personal information.

9. Appraisal

The routine appraisal of records ensures their availability as information assets of the University, provides clarity on the requirements around their retention, assists in finding the right information at the right time, and helps in the identification of underlying information management issues. This process is routinely and regularly conducted by the Business Owners of records, then validated and approved by Records & Archives staff.

A record must never be destroyed without first undergoing a process of appraisal and the approval of the relevant authority. The destruction of a record must always be correctly documented. Records captured to University **Systems of Record** have, through their capture to the system, already undergone a process of appraisal and do not require further action.

Appraisal decisions are made in accordance with the requirements of the *State Records Act 1998* (NSW) including adhering to the General Retention and Disposal Authorities (GDAs), issued by the State Archives and Records Authority NSW (SARA). Records are legally required to be kept for a minimum period of time, as defined under the NSW GDAs and the University's Functional Disposal Authority (FDA). A record that is short-term in nature, such as a duplicate of an existing record, may be destroyed without further recourse under the terms of Normal Administrative Practice (NAP) (refer to section 8.5).

9.1. Records Appraisal Procedure

Appraisal requires Business Owners to directly link the relevant GDA or FDA class to a record to define its minimum legal retention period and to submit this information to Records & Archives for validation and approval.

Records & Archives will then recommend one of two outcomes, **destroy** or **retain**, for which a number of options are available to the business owner. It is important to note that records must never be destroyed without the approval of Records & Archives.

9.2. Destroy

Records will be authorised to be destroyed when minimum required retention periods have passed and they are not subject to:

- current or pending legal proceedings.
- an application for access under the *Government Information (Public Access) Act 2009* (NSW), the *Health Records and Information Privacy Act 2002* (NSW) or the *Privacy and Personal Information Protection Act 1998* (NSW)
- a Government policy or directive not to be destroyed.

The appraisal form will be returned to the business owner with '**Destruction Authorised**'. The business owner may then arrange for their confidential destruction (refer to Section 9.6) and retain the form as evidence of the process.

9.3. Retain

All records required to be retained will be registered to RAMS by Records & Archives staff to enable their retrieval if required, and to document the result of the completed appraisal process.

'**Retain**' advice can result in the following outcomes:

1. **Archives**

   Records that are appraised as having enduring value will be transferred into the custody of the University Archives. This ensures the preservation and effective management of these records so that they can be used in the future. Records that are identified as being Archival are required to be retained permanently by the University. The University Archives will arrange with the business owner for their transfer to the custodianship of the archives when they are no longer required as active records. They will remain accessible to the business owner. For further information, please refer to the **Archives Acquisition Guideline**.

2. **Retain in Unit**

   Records that have not reached their minimum required retention period or are subject to the exceptions identified in Section 4.1, may be securely stored within the business owner until such time as their appraisal will need to be reviewed.

3. **Offsite Storage**

   Those records still required to be retained for a period of time, may be stored offsite at the cost of the business owner until such time as the appraisal process will need to be reviewed.

9.4. Scanning

Where records are required to be retained for an additional period of time, or where a business owner has a business need to retain records that have been authorised for destruction, it may be possible to convert hardcopy records to digital format.

Conversion of records only impacts their format; it has no bearing on the minimum legal period for which they must be retained.

Scanning only offers a means by which to more readily access and store records where there is a demonstrable case for doing so.

Records & Archives can assist units in developing a business case for the conversion of records to digital format, for their subsequent capture to an appropriate business system, and for the requirements around the destruction of the source hardcopy records (see section 9.6) once conversion has been completed.

Please contact Records & Archives for further information: records@unsw.edu.au.

9.5. Normal Administrative Practice (NAP)

Normal Administrative Practice provides a mechanism, under the *NSW State Records Act 1998* (NSW), to enable staff to destroy certain records without the process of formal authorisation described in section 8.1.

This may apply to documents that are considered:

- of short term value (e.g., routine drafts)
- duplicates of other records,
- unimportant (e.g., messages, facilitating instructions and stationery), or
- solicited and unsolicited advertising material.

Staff should contact Records & Archives where clarification is needed. Consideration of any potential enduring value should always be given before implementing NAP.

Records covered by NAP should be securely destroyed by the business owner.

9.6. Confidential Destruction

Following authorisation for their destruction, records may be destroyed through a secure waste disposal service. Estate Management operates a secure destruction process, available to all staff of the University.

It is imperative that records are only destroyed following authorisation and only through the use of a secure, confidential method. Records placed in standard waste processes introduce the risk of the loss of confidential information.

10. Archives

The process of appraisal is especially important for the purpose of identifying records of an enduring nature that may be required to be retained permanently as Archives.

Information on what constitutes a State or a University Archive, and on the process for the donation of Private papers to the University, is described in the Archives Acquisition Guideline.

The University maintains a permanent collection of Archives on-site, stored in specialised conditions to ensure their longevity. Access to these records is available by appointment, the requirements for which are described in the Archives Access Guideline.

11. High Risk and High Value Records

The University is required to identify the systems, records and information needed to support its' high value and high-risk processes. The records of high-risk high value business and the systems that manage them should be identified and documented to enable them to be prioritised and any risks evaluated and managed appropriately. A register of this information is maintained by Records & Archives staff.

Business owners and system owners are required to comply with additional steps to ensure business continuity in the event of a disaster.

This information enables the University to address the risks associated with managing this information, to devise and implement business continuity plans where necessary, and to focus on ensuring best practice recordkeeping principles are followed at all times with this important information.

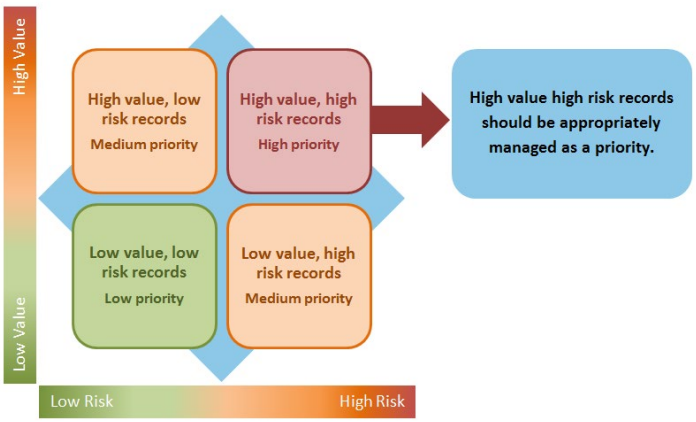


Figure 1: PROV matrix,
https://prov.vic.gov.au/recordkeeping-government/a-z-topics/high-value-high-risk-records

11.1. What are High Risk and High Value Records?

High risk and high value records are one (or more) of the following:

- Records the University is required to retain for more than 30 years
- Records of the University's core activities (research, teaching)
- Records of the University's key corporate functions (personnel, finance)
- Records containing personal information
- Records containing personal health information
- Records of agreements and contracts >$150K (inc. GST)
- Records of significant organisational change

11.2. The Process of Identifying High Risk High Value Records

System of Record evaluations are used to identify where records of high-risk high value business are captured. The completion of these evaluations is the responsibility of the system owner with the support of the business owner.

Senior managers retain overall responsibility for ensuring records of high risk and high value business are safely managed and protected by business continuity plans.

11.3. High Risk High Value Records Register

The register is a listing of those records identified as high-risk high value and the systems that manage them. It is maintained by Records & Archives and can be viewed here.

12. Roles and Responsibilities

12.1. Manager Records & Archives

The Manager, Records & Archives is responsible for the overall management of the University's records and information. Records & Archives are responsible for the maintenance of the System of Record framework, the register of those systems approved for use, and for the promotion of the related processes to all staff. Records & Archives will have oversight of the process of appraisal and provide the necessary approval records of disposal.

12.2. Data & Information Governance Steering Committee

The Data & Information Governance Steering Committee provides oversight for initiatives designed to deliver better outcomes for information across UNSW and input on the strategic management of records.

12.3. Deans/Heads of School/Department managers

Deans/Heads of Schools/Department managers retain responsibility for ensuring:

- appropriate systems and processes are in place for the capture, storage and disposal of records within their areas of responsibility.
- their Unit managers are aware of their recordkeeping responsibilities.
- that Systems of Record are available within their areas for the capture and management of records and that any new systems or process are assessed prior to implementation.
- that business and system owners are aware of the need to appraise records before destruction and to never destroy records without the necessary approval.
- that high risk and high value business records and the systems which manage them are identified and responsibility for capturing and managing these records is assigned.

12.4. Business owners

Business owners retain responsibility for identifying the records of their Unit's activities, the appropriate capture, storage, and disposal of these records, and for ensuring staff are aware of their recordkeeping responsibilities and how to meet them. Business owners must ensure that high risk and high value

business records are captured appropriately to a UNSW System of Record. Business owners are responsible for ensuring that staff are aware of the need to capture records to Systems of Record and that the records of the activities for which they are responsible are captured appropriately. Business owners are also responsible for ensuring identified records of their unit's activities have had a record security classification applied and that records of the activities for which they are responsible are never destroyed without first undergoing a process of appraisal and approval.

12.5. All staff and contractors

All staff and contractors of the University have an obligation to make and keep full and accurate records of their activities and to ensure the secure management of high-risk high value business records using appropriate systems and processes. The University provides training and resources to ensure all staff are aware of these requirements and able to access the necessary tools and systems to meet them. All staff are required to abide by the UNSW *Code of Conduct* to use the University's systems and resources only in the conduct of their official duties.

12.6. System owners

System owners retain responsibility for all records and information captured to the system. They are responsible for the completion of the evaluation of the system prior to implementation and for system re-evaluation in accordance with the requirements based on the Record Classification (section 5). System owners also retain responsibility for all records and information captured to the system throughout its lifecycle including its compliant destruction or migration. System owners are responsible for ensuring systems managing high risk and high value business records are protected by business continuity strategies and plans.

Accountabilities	
Responsible Officer	Director of Governance
Contact Officer	Manager, Records & Archives
Supporting Information	
Legislative Compliance	This Standard supports the University's compliance with the following legislation: *State Records Act, 1998* (NSW) *Evidence Act, 1995* (NSW) *Government Information (Public Access) Act, 2009* (NSW) *Health Records and Information Privacy Act, 2002* (NSW) *Privacy and Personal Information Protection Act, 1998* (NSW) *Children and Young Persons (Care and Protection) Act, 1998* (NSW) *Public Finance and Audit Act, 1983* (NSW) *University of New South Wales Act, 1989* (NSW) *Work Health and Safety Act, 2011*
Parent Document (Policy)	Recordkeeping Policy
Supporting Documents	Archives Access Guideline Archives Acquisition Guideline RAMS Security Guideline RAMS Titling Guideline AS ISO: 15489 Records Management AS ISO: 16175 Principles and Functional Requirements for Records in Electronic Office Environments NSW Standard on Records Management NSW Standard on the Physical Storage of State Records

Related Documents	Cloud Services Guidelines Code of Conduct Data Classification Standard Data Governance Policy Domestic Violence Support Procedure Email Policy Handling Research Material & Data Procedure IT Security Policy Procurement Procedure Report Wrongdoing Procedure Research Data Governance & Materials Handling Policy Third-Party Agreement Recordkeeping Guideline UNSW Guidelines for Commercial Activities
Superseded Documents	Recordkeeping Standard, v1.1 Record Appraisal Procedure, v1.0 Record Security Guideline, v1.0 Record Titling Guideline, v1.0
File Number	2021/045006

Definitions and Acronyms

Business Owner	An organisational role that is responsible for the business oversight of an information system. Business owners of systems are typically senior business operational managers with responsibility for business processes and data/content that are supported by the business system.
System Owner	An organisational role that is responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system.
System of Record	Systems that have been evaluated for their suitability for the capture and management of University records. All University records must be captured to a system of record.
University record	Any document, regardless of format, created or received by University staff in the course of their official duties and kept as evidence of the transaction of business activities.
Data & Information Governance Steering Committee	The Data & Information Governance Steering Committee is the governing body for establishing, maintaining, and promoting the values and behaviours that underpin successful Data & Information Governance at UNSW.
Appraisal	The assessment of University records to determine their retention requirements in accordance with business need and legislative requirements, including the State Records Act (NSW) 1998.

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Manager, Records & Archives	13 December 2017	13 December 2017	This is a new Standard
1.1	Manager, Records & Archives	10 September 2018	10 September 2018	Amended following an internal audit of privacy
2.0	Director of Governance	13 December 2021	13 December 2021	Full review and incorporation of Recordkeeping Procedures and Guidelines.