Staff Recordkeeping Manual

12/09/2017

Records Management Unit
# TABLE OF CONTENTS

## INTRODUCTION ................................................................................. 3

- About the Records Management Unit ........................................... 3
- Our website ..................................................................................... 3
- Contacting the Records Management Unit ..................................... 3

## WHAT ARE RECORDS? ....................................................................... 4

- Why do we need to keep records? .................................................. 4
- How do good recordkeeping help me? ............................................ 5
- How does good recordkeeping help the University? ....................... 5
- What do we need in a record? .......................................................... 5
- Authenticity ..................................................................................... 5
- Integrity ......................................................................................... 6
- Accuracy ....................................................................................... 6
- Completeness .................................................................................. 6
- Accessibility ................................................................................... 6

## TYPES OF RECORDS ........................................................................ 7

- Personal correspondence and documents .................................... 7
- University records ......................................................................... 7
- Permanent records ........................................................................ 7
- Temporary records ....................................................................... 8
- Ephemeral records ....................................................................... 8
- Rough notes and calculations ....................................................... 8
- External publications and advertising material ............................. 8
- Non-circulated drafts .................................................................... 8
- Duplicates and print-outs ............................................................. 9
- Trivial messages and emails ......................................................... 9
- Personal information .................................................................... 9
- Active Records ............................................................................ 9
- Inactive Records ......................................................................... 10
- Vital Records ............................................................................... 10
- Identifying vital records ............................................................... 10
- Creating a Vital Records Register ................................................. 10
- Develop a Vital Records Plan ....................................................... 11

## SCANNING RECORDS ...................................................................... 12

- Reproduction standards .............................................................. 12
- Quality Assurance ......................................................................... 12
- Capturing electronic reproductions ............................................. 13
- Management of the reproductions .............................................. 13
- Destruction of the source records .............................................. 13
- Documentation ............................................................................. 13

## YOUR RECORDKEEPING RESPONSIBILITIES ................................. 14

- The Archives Act 1983 ................................................................. 14
- Responsibilities when outsourcing work ....................................... 14

## CREATING RECORDS ..................................................................... 15

- When should you create a record? ............................................... 15
- What should you include in a file note? ....................................... 15

## CAPTURING RECORDS .................................................................. 16

- Recordkeeping systems ............................................................... 16
- Who is responsible for capturing a record? ................................. 16
Introduction

Welcome to the Records Management Unit's Staff Recordkeeping Manual. This manual is intended to give staff an understanding of the basics of recordkeeping and what they are required to do as employees of the University. After reading this manual, you should be able to:

- Identify the functions and benefits of recordkeeping
- Outline your recordkeeping responsibilities
- Define records and list some of their forms
- Distinguish between types of records
- Describe where to keep records
- Identify where you can find help

This manual is also available in HTML format on the Records Management Unit website at www.utas.edu.au/it/records/support/manual.

About the Records Management Unit

The Records Management Unit (RMU) is part of the Information Technology Services (ITS) section, under the umbrella of the Division of the Chief Operating Officer. The RMU is responsible for the application of good recordkeeping practices across the University, including implementation of the Records Management Policy and Records Management Guidelines.

The Records Management Unit’s mission is to:

- Provide University of Tasmania staff with the tools and knowledge to manage their corporate information (in both electronic and paper format) in a more consistent manner.
- Improve availability and accessibility of business information across all campuses.
- Ensure the University complies with all administrative, legal, fiscal and archival requirements relating to records.

Our website

The Records Management Unit website is located at http://www.utas.edu.au/it/records. If you ever have any questions about recordkeeping, the website is a good place to start looking for the answers, as it hosts a large collection of helpful resources including:

- Policies and Guidelines
- Frequently Asked Questions (FAQs)
- Information Sheets and brochures
- eLearning tutorials (available via MyLO)
- Disposal Schedules
- Forms and templates
- Information on upcoming workshops and other developments at the RMU

Contacting the Records Management Unit

For general enquiries, you can contact the RMU at RMU.Staff@utas.edu.au or call the Manager, Records and Information on (03) 6226 1847. If you need advice about retention and disposal requirements or how to store and manage your records, please contact the Disposal & Training Officer on (03) 6226 1847.
What are records?

What do the following items have in common?

- the minutes of a committee meeting
- a tax invoice
- a signed contract
- a photograph of a workplace hazard

The answer is that they all provide evidence of a business activity, transaction or state of affairs.

Records are "information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business."¹

Records document what we do, when we do it, and why we do it. At their core, records provide evidence that an action or decision has taken place, so that we can prove or discover what happened, when it happened, who was involved, and ideally why it happened.

It doesn’t matter what form a record takes, provided it can be relied upon as evidence of an action or decision. It can take the form of an email, a letter, a spreadsheet, an architectural plan, an audio cassette, or a database entry.

Records allow us to determine:

- what recommendations or advice were given
- who approved an action
- who received a directive and when
- what the instruction/directive was
- whether and when a payment was made

If you’re not sure whether a document is a record, ask yourself:

- Is this evidence of a business transaction or agreement?
- Is this evidence of a decision/policy change?
- Is this evidence of a situation that could result in legal action?
- Does this authorise or approve an action?
- Is this formal advice or a directive/instruction?
- Is this the sole source of information about a particular task or project?
- If I left my job tomorrow, would my successor need this information?

If you answered yes to any of the above, it is a record and must be kept.

Why do we need to keep records?

Records provide evidence of business activities and transactions, enabling the University to operate in an efficient and accountable manner, and ensure that staff members have access to the information they need to do their jobs. Maintaining best practice recordkeeping benefits not just the University, but all staff members, so it is in everyone's interests to use the correct practices.

---

¹ Australian Standard for Records Management (AS ISO 15489:2002), p. 3
How does good recordkeeping help me?

Good recordkeeping helps you find documents and records you need more quickly and easily, saving you time and effort that might otherwise have been spent searching shared drives and desk drawers, and ensuring that you don’t have to make decisions without the relevant documents.

Good recordkeeping:

- Makes it easier for staff to find the information they need, even if the creator no longer works at the University or can’t be contacted.
- Enables staff to check to see if work has already been done in the past or in another department, avoiding reinvention of the wheel and promoting consistency.
- Allows staff to track changes to a document and ensure they have the latest version.
- Ensures that important information isn’t inadvertently deleted or lost.
- Provides evidence of transactions, which can be used to corroborate your claims in a dispute.

How does good recordkeeping help the University?

In addition to meeting its compliance requirements under the Archives Act 1983 and other laws relating to recordkeeping, good recordkeeping helps the University function efficiently and meet the needs of its stakeholders.

Good recordkeeping:

- Ensures that the University meets its obligations under the law.
- Promotes good decision-making and policy formulation by ensuring that managers have access to the information they need to make informed decisions.
- Promotes consistency and accountability in decision-making and service delivery.
- Supports the University in court by providing evidence of transactions and minimising the costs and risks of legal discovery.
- Protects records from accidental or malicious damage or alteration.
- Minimises the disruption caused by disasters by protecting important information needed to continue essential business operations.
- Documents the University’s various activities, policies and achievements, and provides a historical record for future researchers.

What do we need in a record?

Although anything that documents an event or action is a record, to be useful as evidence, we must be able to rely upon it and it must be in an accessible and usable form. Good records must therefore possess the following characteristics:

Authenticity

Authenticity means that it can be proved that the record:

- is what it purports to be
- was created or sent by who it claims to have created or sent it
- was created or sent when it claims to have been created or sent.

In the past, the authenticity of a record was usually demonstrated through the use of seals, signatures and date stamps, but in the modern era of scanners and Photoshop, these measures have become less effective, especially when dealing with electronic records. The best ways to establish the authenticity of electronic records are by using digital signatures (i.e. asymmetric encryption keys, not mere scanned signatures) to establish the identity of the sender and capturing records in a recordkeeping system with their metadata to establish the date and time.
Integrity

Integrity means that the record has been protected from unauthorised access and tampering throughout its lifespan, and can be proved to be complete and unaltered. This is best achieved by lodging the record in a secure recordkeeping system with restricted editing permissions. A record with integrity is also sometimes described as inviolate.

Accuracy

An accurate record is one that can be relied upon as an accurate account of the discussion or event that it documents. Note that a record can be both authentic and inviolate, but still be inaccurate due to faulty recollection.

Accuracy can be maximised by creating records at the time of the event or as soon as possible afterwards, while memories are still fresh, and by checking all participants agree that it is an accurate depiction of events.

Completeness

For a record to be useful, it must contain enough information to give a complete picture of events and the surrounding context. This can be done by ensuring that the whole document is captured along with metadata (e.g. author, date, title etc.) and links to related records.

Accessibility

An accessible record is one that can be readily located, retrieved and understood by people who were not directly involved in the events documented. It must be stored in a readily accessible format and be free of jargon and acronyms. It must be stored in a system that makes it readily accessible to everyone who requires access to the information, along with descriptive metadata to make it easy to find.
Types of records

Personal correspondence and documents

Although personal correspondence and documents may be records of your private business dealings, they are not University records and you are not required to keep them under the *Archives Act*. However, if a document or email contains information relating to University business, it must be treated as a University record even if it is otherwise of an informal or personal nature. We therefore encourage you to keep work and social emails separate.

University records

University records (aka corporate records or business records) are records relating to the business activities of the University of Tasmania.

The University owns all records created and received by individual employees as part of their day to day business, including research data, teaching materials and correspondence. Under the *Archives Act 1983*, the University's records are State Records and must be managed and disposed of in accordance with the Act.

Obviously not all University records are of equal value, and they fall into three basic categories:

- **Permanent records**, which have long-term value and must be kept for 25 years before being transferred to the Tasmanian Archive & Heritage Office.
- **Temporary records**, which are of medium-term value and must be kept for a finite period of time designated by the State Archivist before they can be destroyed.
- **Ephemeral records**, which are of little or short-term value and can be freely destroyed.

You can determine which category a record falls into by looking it up in the disposal schedules authorised by the State Archivist, which describe various classes of records and their associated disposal categories and retention periods.

Permanent records

Permanent records are records that are deemed to have long-term value even after their immediate value as evidence of business activities has faded, usually for their potential historical value.

Examples include records that:

- provide evidence and information about the University's policies and actions
- provide evidence and information about the University's interactions with its students
- document the rights and obligations of University staff and students
- contain evidence and information about activities of interest to stakeholders
- have significant potential research value

Permanent records must not be destroyed! Instead, they must be retained for 25 years, after which they must be transferred to the Tasmanian Archive & Heritage Office for incorporation into the State Archives. You may apply to the TAHO for permission to retain the records longer than 25 years if they are required for business reasons, or conversely, apply for earlier transfer, though the latter is unlikely to be approved given current storage constraints at the TAHO.

To transfer permanent records to the TAHO, you will need to list the records and their disposal classes in an Application to Dispose of State Records and submit it to the TAHO. The RMU will be happy to provide advice and assistance if you need help. Before transferring the records, you will need to prepare them by removing any staples or metal paperclips (these can leave rust marks) and placing them in an archival quality acid-free box (these can be ordered from Archival Survival or Zetta Florence), along with a box list.
Temporary records

Temporary records are records that provide evidence of important business activities but are not deemed to have any long-term value once they are no longer needed for that purpose.

They must be kept for a finite retention period identified in an authorised disposal schedule, after which they can legally be destroyed. Note that this is only the legal requirement: subject to privacy requirements, you may retain temporary records after their retention period has expired if you wish to retain them to meet business needs.

Before destroying any temporary records (apart from ephemeral records), you will need to submit a Records Destruction Request form to the Records Management Unit for approval, describing the records you wish to destroy and citing the disposal classes you believe authorise the destruction of the records.

Ephemeral records

Ephemeral records (a.k.a. short-term-value records) are records that are used to facilitate University business but that are of a trivial nature or used solely in the creation of more significant records. Ephemeral records do not need to be saved into a recordkeeping system.

These records are considered to be of such low or short-term value that they may be routinely destroyed without the need to list them in a Register of Records Destroyed, unless they:

- were created before 1960;
- relate to an ongoing or imminent government investigation or inquiry;
- relate to an ongoing or imminent court case, Native Title claim or Right to Information request; or
- document links between indigenous peoples, communities and sites.

If any of these apply, please contact the Records Management Unit for advice.

The destruction of ephemeral records is authorised in DA 2158: Short-Term-Value Records, which provides a full listing of the types of records that can be considered ephemeral, but the most common examples are described below.

Rough notes and calculations

Working papers, background notes, audio recordings, reference materials, spreadsheets and calculations used solely in the preparation of other records such as correspondence, reports, budget documents, programs and tabulations.

External publications and advertising material

Records and publications from outside sources that are kept solely for reference, such as invitations to functions, copies of other university annual reports, unsolicited promotional literature for goods and services, catalogues and published documents.

Non-circulated drafts

Sometimes we need to track the development of a document over the course of time, capturing records of what the document looked like at key points in its development.

A draft or new version of a document must be captured as a record if it:

- was sent to others for comment or approval;
- provides evidence of approval/rejection in the form of annotations;
- contains significant information not contained in the final document;
- shows the context and/or content has changed significantly; or
- has ongoing value for business reasons, e.g. it provides a way to track and document a development or decision-making process.

Drafts that don't fall into any of the categories listed above are ephemeral records and can be freely destroyed, i.e. you don't need to keep every minor draft documenting formatting changes or fixing typos and spelling errors.
You only need to capture annotated drafts separately if they represent comments, feedback or instructions intended for someone other than the person making the annotations. Annotations in the form of personal notes are not considered significant enough to capture as a separate version, nor are minor annotations such as correcting spelling or grammar.

**Duplicates and print-outs**

The University only needs to keep one official ‘master copy’ of each record, with excess copies being considered ephemeral records that can be freely destroyed. These include duplicate copies of minutes, agendas, copies of internal circulars and publications, copies of financial records maintained for convenient reference and reference copies of film, video, microfilm or microfiche.

If there are multiple identical copies of a record, such as minutes of a meeting, one copy must be designated as the master copy and captured in a recordkeeping system. Ideally, the others should be explicitly marked as duplicates using a "COPY" stamp in the case of physical records, or using metadata and/or an electronic watermark in the case of electronic records.

Print-outs of information stored in an electronic recordkeeping system such as TechOne are also effectively duplicates. If you can establish that the master copy of a record is stored in a University recordkeeping system, then you may destroy any exact duplicates or print-outs of that record under DA 2158.

The master copies of certain records are centrally maintained by the business areas responsible for those functions and other University business areas may therefore dispose of any duplicates of those records they hold. A full listing of the types of records that fall into this category will be included in the planned Retention and Disposal Guide for Schools and Faculties, but in the meantime, staff are asked to confirm with the relevant business areas that the records in question are in fact duplicates of master copies held by the business area.

Key business areas currently holding the master copies of common records include Financial Services, Human Resources and the Student Centre.

**Trivial messages and emails**

Transmittal messages and other trivial messages which do not record University business transactions or formal communications between staff members are also considered ephemeral and may be freely destroyed. Examples include:

- informal transmission messages on ‘with compliments’ slips;
- email and facsimile cover notes;
- facsimile or telephone messages of a routine or trivial nature;
- letters of appreciation and greeting cards; and
- informal emails and instant messages.

If you are unsure whether a message is trivial or not, ask yourself whether it is evidence of a transaction, agreement, policy change/decision, formal advice or a directive; authorises an action; relates to a matter likely to be reviewed or audited; or contains information your successor would need if you were to leave your job tomorrow. If none of these apply, then the message may be considered trivial and may be destroyed under DA 2158.

**Personal information**

Documents containing personal information acquired by the university which are not required on a continuing basis to support the business transactions to which they relate, e.g. copies of birth certificates, drivers’ licences, marriage certificates, copies of references, copies of qualifications, change of address notices.

**Active Records**

Active Records are those records that are in active use or likely to be needed on a frequent basis. Active records can include records deemed permanent, temporary, vital or ephemeral.
Inactive Records

Inactive records are records that are no longer utilised on a day-to-day basis but must be kept for business, legal or legislative reasons for a specified period of time. Inactive records are often relocated to a storage area (an archive) where they can be safely kept until they can be legally destroyed or transferred to the Tasmanian Archive and Heritage Office in accordance with University disposal procedures.

Vital Records

Vital records are those records without which the University could not continue to operate and “contain information essential to effectively restore business operations during or following an exceptional event (e.g. network failure, a disaster)”\(^2\). They typically represent between 5-10% of University records.

Records can be divided into four categories of business value:

- **vital records**: those which are critical to operations and may be extremely difficult to replace, or incur a significant cost to reproduce
- **important records**: could be recreated with some level of resources
- **useful records**: would cause some inconvenience if lost but are replaceable
- **non-essential records**: those which would not cause any impact to operations if lost (e.g. records relating to the publicising of past events or services organised by the agency or records due for disposal under an approved Retention and Disposal Schedule).

Vital records can be temporary records or permanent records: what makes a record vital is how critical it is to business operations *right now*, irrespective of what its value may be in the future. The category a given collection of records falls into can (and often does) change over time, with most vital records being active records. For example, an agreement may be a vital record while it remains in force, then becomes merely useful or non-essential once it expires.

Examples include records that contain information critical to:

- emergency preparation and response
- core business operations (i.e. critical client services)
- protecting the legal and financial rights of the University
- protecting the legal and financial rights of students and University clients

*Identifying vital records*

The first step in identifying your vital records is to identify your business area’s critical business functions and mission critical operations. Which business processes are essential to the functioning of the University? Which records are absolutely essential to performing these operations on a day to day basis, without which work would come to a stop? Is the information contained in these records replicated any in other records or systems? If so, how difficult and time-consuming would it be to retrieve this information in order to resume operations?

*Creating a Vital Records Register*

Once you have identified your vital records, they should be registered in a Vital Records Register. You can find a template [here](#). We are also developing a University wide Vital Records Register which you will be able to contribute to through a web form on our website. The following details should be included for each record:

---

\(^2\) TAHO Advice 52: Identifying and Managing Vital Records
Develop a Vital Records Plan

Beyond registering your vital records in a Vital Records Register, it is also important to develop a plan for protecting your vital records. This should include a risk management assessment of the various risks posed by natural disasters, industrial accidents, human error and malicious damage, and a plan for recovering vital records in the event of a disaster.

Risk Management Assessment

This should be carried out in accordance with Australian Standard 4360-1999 and University guidelines. You should assess both the likelihood and consequence of each risk on a matrix. For examples, see the matrix on the second worksheet of the Vital Records Register template.

You will need to consider:

- physical risks to storage areas for physical records
- physical risks to hardware hosting electronic records
- connectivity risks for externally hosted electronic records
- security risks to electronic records

Some of the risks to be considered include:

- Flooding of physical storage areas or server rooms (from storms, floods, burst pipes, sprinkler malfunction)
- Fire (electrical, chemical, bush fires, lightning strikes)
- Ransomware and other malicious hacking attacks
- Connection problems with externally-hosted documents and systems (e.g. in the Cloud)
- Accidental loss through human error

Prioritise the risks in terms of the acceptability of the overall risk. The next step is to consider the options for preventing or minimising those risks. It may not be possible or cost-effective to entirely prevent some risks, in which case you will need to consider strategies for minimising the likelihood and/or impact of the risk and for recovering if it does occur. Some examples of preventative measures include relocating records stored in risky storage areas, engineering solutions to reduce or eliminate hazards or protect records, backing up electronic records, creating access copies of records and storing the originals in a secure off-site location, and instituting procedures to minimise risks.

Disaster Recovery Plan

You will also need to either draw up a disaster recovery plan, or if one already exists, ensure that it includes a section dealing with the recovery of physical or electronic vital records that have been damaged or become temporarily inaccessible. Whether that means repairing damage, restoring access to externally hosted records or finding alternative sources for the information, the core objective is the same: to restore access to the information needed to resume operations as quickly as possible. This may require the implementation of temporary emergency measures, in which case the secondary objective is to ensure continued access to information in the medium to long term, once any emergency measures have been removed.

For more information, see State Recordkeeping Advice 52: Identifying and Managing Vital Records.
Scanning records

Business areas frequently ask whether they need to keep the original paper copies of records they have scanned and saved in digital format (e.g. PDFs and TIFFs). In the vast majority of cases the answer is yes, you will need to keep the originals. While it is technically possible to destroy the originals under the authority of DA 2159, this disposal schedule and the associated State Records Guideline No. 8 impose strict requirements on the process that most University business areas will find very difficult to meet.

To destroy the paper versions of records you have scanned and captured as electronic records under DA 2159, you will need to set up a rigorous digitisation program in consultation with the Records Management Unit. This will involve a considerable investment of time and resources to put in place the appropriate procedures, quality assurance checks and training.

Reproduction standards

The scanned records must be functionally equivalent to the source records, being complete and accurate reproductions that have the degree of accessibility and useability necessary to substitute for the source records.

In practical terms, you need to ensure that:

- no pages are omitted (especially when scanning double-sided documents);
- the pages are in the correct order;
- all the information on a page is accurately copied;
- handwritten comments and signatures are legible;
- text isn’t cut off or made indistinct by the edge of the page;
- text in shaded or highlighted areas is readable;
- diagrams, graphs, tables and photos are clear and distinct;
- colours important to understanding the information are accurately reproduced (consider using a target sheet to check colour reproduction);
- records are scanned at a resolution of at least 300 dpi (600 dpi for photos);
- records are encoded using a lossless format (e.g. PDF/A, PNG or JPEG2000) to avoid distortion and loss of information;
- copies are accompanied by sufficient metadata to provide context and meaning, and to demonstrate the authenticity of the record.

Quality Assurance

A compliant digitisation program must have comprehensive quality assurance and verification procedures in place to ensure that no information is lost. Responsibility for each step of the digitisation and verification process must be clearly assigned, and those responsible trained in the necessary procedures. Verification should be undertaken by someone other than the scanner operator.

The source records will need to be retained long enough for the verification to take place (we recommend at least six months), and there will need to be procedures to ensure that the source record is not damaged or altered by the copying process in order to ensure it can be used for verification. If any defects or errors are detected, the document will need to be rescanned.

There should also be monthly tests and audits of the equipment and processes, with the results recorded in a recordkeeping system. An annual review of the program should be conducted to identify and respond to issues of concern.

The procedures should cover at least the following:

- Allocation of responsibilities and authorisations for different processes/aspects of the program
- How to prepare documents for scanning and what to do with documents that may cause scanning difficulties, such as photocopied documents, stapled documents, and spiral or glue bound documents
- Document batching
- Calibration, use and checking of the scanning equipment and software
- Which metadata must be captured through OCR or manual data entry
- Checking accuracy of data from OCR and manual data entry
• Scanning processes to ensure all documents and all pages are scanned
• Creation and use of a sample set and criteria
• Quality control benchmarks
• Evaluating image quality
• Rescanning and correcting errors
• Acceptable output formats
• Restrictions on the use of image processing (e.g. de-speckling)
• How long source records should be retained for verification purposes
• Documentation of the digitisation process
• Destruction of source records

Capturing electronic reproductions

The main stumbling block for many business units will be the requirement in State Records Guideline No. 8 to capture the scanned reproductions into an electronic recordkeeping system before the original records can be destroyed.

Some business units have access to HPE RM, the University’s preferred recordkeeping system. As a fully featured Electronic Document and Records Management System (EDRMS), HPE RM is designed to meet these requirements and business units with HPE RM access can comply with this aspect of Guideline No. 8 by capturing all scanned records into HPE RM.

Unfortunately, not all business units have access to HPE RM and these business units will find it more difficult to comply. Many currently store their electronic records on shared drives, which do not meet the requirements of a formal recordkeeping system. There are some business information systems that meet the requirements, such as TechOne Financials, and these can be used to capture electronic reproductions, but most systems currently available do not.

However, even if you can’t meet the requirements to destroy the original records, in some cases it may still be worth scanning the records to create electronic copies for everyday use and storing the original paper records off-site until they are eligible for destruction.

Management of the reproductions

Remember that in replacing the original source records, the reproductions will become the official records. You must ensure that the reproductions are kept for the authorised retention period that applied to the original records. If destroyed, they must be listed in a Register of Records Destroyed. If the original records were permanent records, then the reproductions are also permanent records and must be retained for 25 years from the creation date of the original records, after which they must be transferred to the Tasmanian Archive and Heritage Office.

Destruction of the source records

The source records must be retained for verification purposes until the quality assurance process has been completed and the reproduction lodged in a recordkeeping system, after which they may be destroyed using a secure destruction method such as cross-cut shredding or locked shredding bins.

As the reproduction is now the official record, source records are not listed in a Register of Records Destroyed. However, the destruction date of the source record should still be recorded in the metadata attached to the reproduction and/or a register of digitised records, as this information may be required in the event of a legal discovery request.

Documentation

Finally, business units will need to document the digitisation process to record:

• Who was responsible for the scanning and verification of a record
• Which source records have been converted
• If and when the source records were destroyed
• When the reproduction process occurred
• What equipment and processes were used
• What policies and procedures were in place and whether they were followed
• The results of tests and audits
Your recordkeeping responsibilities

You must:

- keep complete and accurate records of activities relating to your work
- create records of important verbal discussions such as meetings and conversations
- capture records in an appropriate recordkeeping system
- give records and folders meaningful titles
- dispose of records appropriately and in accordance with the law
- manage records in accordance with the Records Management Guidelines
- ensure that recordkeeping clauses are included in outsourcing contracts

You must not:

- destroy, delete or alter records without authorisation
- lose records in your care
- remove University records without permission
- provide restricted records to unauthorised persons

The Archives Act 1983

The Archives Act 1983 is the primary piece of legislation governing recordkeeping in Tasmania.

As a body established by an Act of Parliament (the University of Tasmania Act 1992), the University of Tasmania is a State Authority and its records must be managed as State Records under the Archives Act.

Under the Act, all University employees are responsible for creating and keeping records of actions and decisions they take in the course of their work for the University, including interactions and transactions conducted with external parties. Breaching these responsibilities could lead to prosecution and fines of up to $5000 per breach.

Don't worry, you don't need to read the Archives Act itself, as all the requirements are laid out in the Records Management Guidelines. The key point to remember is that it is against the law to destroy the University's records without the State Archivist's authorisation (usually obtained via an approved disposal schedule).

Responsibilities when outsourcing work

Any records created in the course of work performed on behalf of the University are University records and therefore State Records under the Archives Act, whether the work is performed by a member of staff, a consultant or contractor, or outsourced to a company.

It is essential that consultants and contractors are made aware of their recordkeeping obligations and that you include clauses regarding ownership, access, storage and disposal of records when drawing up contracts. See State Records Guideline No. 10 for more information.
Creating records

When should you create a record?

In many cases, records of business activities and transactions will be generated as an inherent by-product of the activity or transaction, which can then simply be captured and kept as a record of the activity or transaction. For example, if you receive an important email or signed contract, that email or contract is the record and should be captured as such.

However, sometimes important decisions or agreements will be made verbally in a meeting or over the phone, where there will be no email or memo to capture, in which case you will have to actively create a record of the discussion/events to capture. The classic example is taking minutes of a committee meeting, where the taking of minutes during the meeting is typically routine and formalised, but it may also be necessary to document an ad-hoc meeting or telephone conversation after the fact. You may also wish to transcribe voice mail messages if they record directives or approvals.

In general, you should create a record of any verbal discussions that produce:

- agreements
- transactions
- decisions
- orders/directives
- formal advice or recommendations
- approvals and authorisations

The best way to record these discussions is to formalise them via an email recapping the conversation and capture the email conversation, but you can also take minutes or write a file note to be circulated and signed by all participants, and capture that.

Memory is notoriously unreliable, so send the formal email or create and circulate the file note as soon after the event as possible, while it is fresh in everyone's minds. When circulating a file note, it is advisable to retain a copy for yourself in case the circulated copy is lost.

Another situation in which it may be necessary to create a record is when you witness an accident, incident or hazardous situation. This can be documented via an email or file note, possibly supported by photographic evidence.

What should you include in a file note?

There is a template available on the Records Management Unit website, but you can use pen and paper, a Word document or another format provided you cover the following points:

- What was discussed?
- Were any decisions or agreements reached?
- Who were the participants?
- Who wrote up the notes?
- When did the discussion take place?
- When were the notes written?
Capturing records

Capturing a record means preserving a complete and fixed impression of the information as it existed at a particular point in time, much as people sometimes refer to capturing a transitory moment in a photo. By capturing a snapshot of a document as a record, we can go back later to see what it looked like at the time it was captured, even if the document has been altered since.

We capture a record by "lodging [it] in a recordkeeping system and assigning metadata to describe the record and place it in context".3

In order to guarantee that the captured record is an accurate representation of its condition at that point in time, it is important to capture the record and its metadata as close to the time of creation or receipt as possible.

If a delay occurs, continuity and contextual information is often lost, reducing the evidentiary value and usefulness of the record. This can make it harder to establish the integrity of a record and can hinder decision making processes, especially if it affects other areas of the University.

Recordkeeping systems

Records that are in active use should be stored in a recordkeeping system, so that they can be easily found and retrieved by any authorised staff member who needs to access the information.

A recordkeeping system is a system that:

- Capturing records and their metadata
- organises records to make it easy to find and retrieve information
- makes records accessible to all authorised persons who need access
- protects records from unauthorised alteration and destruction
- incorporates security and access controls
- provides an audit trail to track who accesses and/or edits a record and when.

Who is responsible for capturing a record?

Although we'd rather you erred on the side of caution, there is no need to capture a record more than once. The general rules here should generally stand you in good stead, but if in doubt, check the recordkeeping system in use at your business unit to see if someone else has captured the record, and if not, capture it yourself.

- If it was created by a University employee, then the record's creator should capture it.
- If it was created by an external party, the employee who received the record should capture it. If there are multiple recipients, the employee chiefly responsible for the issue should capture it.
- Even if you are not responsible for capturing a record you've received, it's still good practice to check whether it has been captured to make sure it doesn't slip through the cracks.
- If you have HPE RM access and the other employees who sent/received the record do not, please capture a copy of the record in HPE RM, even if one of them would normally be responsible.

3 (National Archives of Australia, n.d.).
Titling records

It is important to take care when titling records. Remember, although you might know where to look now, you might not remember in a year's time, and if the title isn't meaningful and precise enough to distinguish it from similar or related records, you might end up wasting a lot of time searching through documents to find what you are looking for. If a colleague needs to find it, they will probably find it even more difficult.

**Titles should be meaningful**

A title doesn't have to be lengthy to be meaningful, but it needs to include sufficient information to make it clear what the record is about and to enable it to be easily found. Think about the kind of search terms you might use if you were searching for it.

**Distinguish records from similar or related records**

Make sure the title is specific enough to differentiate it from similar or related records. Try to be as precise as possible in defining the subject and keep the likely titles of similar records in mind.

**Avoid vague terms such as ‘miscellaneous’ and ‘various’**

It may be tempting to use vague terms such as "miscellaneous", 'other', 'various' or 'general correspondence', but these words are next to useless as search terms, forcing people to wade through a large collection of random unrelated documents to try and find what they are looking for. Try to be as specific as possible.

**Avoid using acronyms and abbreviations**

Abbreviations and acronyms can be very convenient, but they can cause problems with retrieval when people are searching for records, and should be avoided when titling records.

Not everyone uses the same abbreviations and people searching for a record using the full version of a word may not find it if it uses the abbreviated version. You must use the full version of the word when titling records.

Acronyms can be meaningless to colleagues from different areas and often lose their meaning over time as organisations evolve and business units are merged, dissolved or change their names. Therefore, you must use the full version of the acronym when titling records. If people are likely to search for the acronym, you may include it in parentheses after the expanded version.

There are a few exceptions to this rule, such as the acronym "UTAS" itself. For a list of acceptable acronyms and abbreviations, please see the [Data Entry Standards](#).

**Titles should be consistent**

Titles should be structured and formatted consistently to make it easier to find records and to distinguish between drafts and different versions of the same document. This also applies to the formatting of dates (e.g. YYYY-MM-DD for filenames), ordinal numbers (first vs 1st) and numerals (4 vs four).
Managing physical records

Humanity has been keeping records for thousands of years, and for the vast majority of that time, did so without the help of computers.

While the volume of information produced has dramatically increased in recent decades, much of this is ephemeral and the traditional techniques are still quite capable of managing the far smaller number of significant business records, especially when augmented by basic computer aids such as spreadsheets.

Furthermore, although most records created today are created in electronic format, most business areas still have significant collections of legacy records in paper format and continue to create some records in paper format (e.g. forms). In most cases, it is not practical or cost-effective to digitise these records, so they must be managed in a paper-based recordkeeping system.

Active vs. inactive records

Active records are records that are still in active use or likely to be needed on a frequent basis. Inactive records are records that are no longer utilised on a day-to-day basis but must be kept for business, legal or legislative reasons for a specified period of time. Inactive records are often relocated to a storage area (an archive) where they can be safely kept until they can be legally destroyed or transferred to the Tasmanian Archive and Heritage Office (TAHO) in accordance with University disposal procedures.

Organising paper records

Records should be grouped by business activity (e.g. enrolment) rather than by organisational unit or by project, as this will enable you to dispose of records at the folder level, rather than have to appraise each individual record in a folder. The files should be stored in a logical order. In some cases (e.g. student files), it may be logical to order them alphabetically or by academic semester, but we recommend using a simple sequential number with a year prefix (e.g. 14/1234) to avoid the need to leave gaps or move files to make room for new files.

Tracking paper records

As some inactive records must be retained by the University for a lengthy period of time, steps must be taken to ensure that there is a record of what information is stored and where it is held. If this is not done, then it often causes problems down the track, when inactive records are using up valuable storage space but the staff members responsible have long since moved on, making it difficult to ascertain the value, relevance and context of the records.

This means someone has to go through each item to establish what it is and whether it is an original or a duplicate. This investigation process is very resource intensive, and some pre-planning and the adoption of good recordkeeping practices can save you a lot of time and effort in the long run.

If you have HPE RM, you can track records by creating HPE RM entries for each folder and box and updating their location details. If not, you will need to create a Register of Inactive Records spreadsheet listing all your inactive folders and where they are. Store it on a shared/network drive where everyone in your workgroup can access it. A template is available from the RMU website.

Create an entry for each folder, listing the title/description, date range, the number/barcode of the box and the storage location (or file path if electronic). It should also identify the disposal class (if scheduled), the retention period, and if they are temporary or permanent records, so you can dispose of the contents once the retention period has expired. The Register should be periodically checked to determine whether any records are eligible for destruction or transfer.

Other details such as project numbers may also be listed to facilitate retrieval. This will enable staff to search for the appropriate entry in the index and then locate the physical folder using the folder number.
Storage containers

Paper records should be stored in clearly labelled and numbered files, preferably secured using plastic tube-clips, as these make viewing, adding, removing and photocopying the contents of the file easier and don’t leave rust marks or break as easily as lever-arch files and ring binders.

Temporary records should be stored in good quality heavy-weight manila folders or lateral files (white or buff). Permanent records should be stored in archival quality acid-free lateral files. Reinforced colour tabs are recommended to identify the originating area/division/section. Alphanumeric colour-coded labels help identify misfiled folders. Lateral file fasteners/tube-clips make viewing, adding, removing and photocopying contents of the file easier.

Files containing records in active use should generally be kept in lockable lateral filing cabinets or in open shelving bays in a secure but accessible storage area.

Files containing inactive records can be stored in boxes: temporary records can be stored in sturdy archival boxes such as those sold by commercial storage providers, but permanent records will need to be kept in Type 1 (17x25x38cm) acid-free archival boxes. Number or barcode boxes so that retrieval is easier.

When boxing, group similar disposal classes of records by the destruction or transfer date if possible, as this will reduce costs and double handling of boxes. Use good quality boxes and don’t overfill them. You should be able to retrieve or replace papers/folders easily without damaging papers, the box or your hand.

Storage areas

Physical records should be stored in a secure (e.g. locked or swipe access) storage area with the appropriate environmental conditions. It should be located away from water pipes, electrical plants and other fire hazards, kitchens and toilets. It should have good drainage, no direct sunlight, and should be well ventilated and kept free of dust and pests.

It is generally advisable to have separate storage areas for active records (i.e. records that are frequently required) and inactive records (i.e. infrequently required records). Storage areas for active records should be centrally located or at least easily accessible, so that staff can readily retrieve any records they need. Storage areas for inactive records can be more remote.

The University does not have a central repository for inactive physical records. It is the responsibility of each Section, Faculty, School or Institute to store and maintain its records until they can be destroyed or transferred to the TAHO.

Regardless of where you store inactive records, you will need to maintain a Register of Inactive Records cataloguing and describing the content of boxes and folders, where they are kept, how long they need to be kept, and a barcode or box number.

Off-site storage

If your business area doesn’t have access to any suitable storage areas on campus, you can store inactive records off-site at one of the storage companies recommended by the RMU: GRACE Records Management or ZircoDATA.

Both maintain specialised storage facilities in the Hobart area (though they service all of Tasmania) and provide various levels of service to assist you in storing your inactive records in a controlled environment. They also offer a variety of services including scanning, cataloguing and boxing.

The storage costs of inactive records that are stored with RMU recommended commercial storage providers are paid for centrally. If business areas choose to store inactive records in other facilities, it is at their own cost. All storage facilities must comply with State Records Guideline 11 - Physical storage of state records and State Records Guideline 13 - Certification for secondary storage providers.
All service charges including boxes, transport, deposit and retrieval, scanning and disposal will be the responsibility of the business area. The service charges will either be separately invoiced by the provider or a University Internal Transaction (UTRAN) will be created.

Consider the type of records you will be placing off-site, how long you need to keep them and how often you may require access to these records. The collection and delivery charges used by commercial storage providers vary, so carefully consider your requirements before selecting a provider. If the records are recalled regularly, it may not be cost-effective to store them off-site.

If your business unit uses HPE RM, your HPE RM Liaison Officer will need to register the boxes and enclose their contents in HPE RM so the records can be tracked and retrieved. You will also need to attach a barcode sticker (these are provided by the storage companies) and enter the barcode in the Storage Provider ID field of the box's HPE RM record.

If HPE RM is not available in your business unit, all inactive records must be listed in a Register of Inactive Records prior to transfer, including identification of the disposal class, status and date range. Send a copy of the Register of Inactive Records to the Records Management Unit once the records have been transferred to the off-site facility.

Contact the Records Management Unit to assist in coordinating the transfer and arrange a cost account to be set up for your business unit if you haven’t deposited records off-site before. This will allow monitoring of the number of boxes stored off-site and will also allow service charges to be costed to the correct business unit.
Managing electronic records

HPE Records Manager (HPE RM)

HPE Records Manager (HPE RM) is an Electronic Document and Records Management System (EDRMS) which captures, manages and provides access to records and information through time. HPE RM has the capacity to manage all business information including administrative, research, teaching and course material regardless of format.

HPE RM includes a classification scheme, disposal & retention functionality, a contacts database and the ability to track information across the University. It also has the capacity to integrate with other business systems such as SharePoint, the Research Management Data Base, TechnologyOne Financials, and the Human Resources Management System.

It is the University’s preferred recordkeeping system, but is currently only available in a few key business areas. Other business areas may request HPE RM using the Application for HPE RM Access form, but should be aware that HPE RM is currently rolled out to new business areas on a case by case basis.

A business case is required to substantiate the need for a roll-out to an additional area and a formalised project will be set up to support planning and implementation. Please note that the Records Management Unit has limited resources to implement and support large installations, so consultants may need to be engaged to assist with business analysis, configuration and training.

Business Information Systems

There are a number of business information systems in use at UTAS, such as TechOne, the Research Management Database and Archibus. Some of these (e.g. TechOne) possess the requisite functionality to be used as a recordkeeping system, but most lack key features such as audit trails or are too narrow in their focus to be used as recordkeeping systems.

Wikis

According to Wikipedia (the world’s most famous wiki), a wiki is “a website which allows its users to add, modify, or delete its content via a web browser”⁴. They are designed to facilitate and promote collaborative work by making it as easy as possible to create, edit and link pages via hyperlinks.

While public wikis such as Wikipedia can be read and edited by anyone, internal wikis such as the University of Tasmania Wikis allow viewing and editing permissions for a given page (or group of pages, known as a space) to be restricted to staff from certain business areas or user groups. This makes them useful repositories for business areas’ documents and knowledge. The University’s Wikis use an enterprise wiki platform called Confluence.

Although internal wikis are not true recordkeeping systems, if you don’t have access to HPE RM, then they are probably the best option for storing electronic records and they have a number of advantages over shared drives:

- Wikis have inbuilt revision histories that automatically store past versions of both wiki pages and any attachments, adding a new revision each time a page is edited or a new version of document is attached, and logging who created or edited pages or attachments.
- Records are automatically protected from deletion, though protection is lacking compared with HPE RM.

---

• Wikis make linking documents easy, which makes them excellent for linking related records.
• It is easier to set and tailor security permissions for wikis than shared drives.
• Automatic capture of some metadata (title, date registered, date modified, registered by, last modified by), though not as comprehensive as HPE RM.

However, wikis do have some notable shortcomings as recordkeeping systems:

• Lack of recordkeeping functionality, meaning that the authenticity and integrity of records cannot be established to the degree necessary to be able to rely upon the record as evidence.
• Users with permission to edit pages can create pages and vice versa.
• They don’t capture all the necessary metadata, such as author, creation date, software application, or details of changes to access permissions.
• They are often poorly organised, which can lead to duplication and make it hard to find records or determine which version is the most current.

Not much can be done about the first two points, but the metadata can be improved by filling out the document properties fields in Microsoft Office and Adobe Acrobat etc., and the implementation of a controlled folder structure will make it easier to organise records and prevent duplication.

The most important step is to organise your business area’s wiki space into a logical structure based on business functions and activities and to implement controls such as restricting the ability to create new pages, to avoid the proliferation of unstructured pages such as “Jane’s documents” or “Miscellaneous”, which can make it difficult to locate records and lead to problems with duplication and version control.

We strongly recommend basing your folder structure on the University’s Business Classification Scheme, as this will not only provide a consistent and logical structure, but will also ensure that your records are grouped together by disposal class, which will make it much easier to dispose of records.

It is also important to provide clear guidelines and training in how and where to store and retrieve records from the wiki, how the folder structure works, and which formats to save records in. Although wikis are designed to be as easy to use as possible, some training may be required, especially for those staff who will be given administrative rights and responsibilities for the wiki.

Contact the Service Desk for assistance in setting up a wiki for your area.

Shared/Network drives

A shared drive (also known as a network drive) is an electronic storage space hosted on a shared server where staff can store electronic records such as PDFs, Word documents, Excel spreadsheets and images. They are sometimes referred to by their drive letter, e.g. “N:" drive.

Shared drives allow authorised users to access and share files with the rest of their business area by providing a central repository that can be accessed regardless of whether a colleague’s computer is turned on, facilitating collaborative work and the sharing of information. They can even be accessed remotely via a Virtual Private Network (VPN). Unlike hard drives, they are regularly backed up by IT Services, reducing the risk of losing documents.

Shared drives are probably the most commonly used storage location for electronic records, but they have a number of drawbacks that make them less than ideal recordkeeping systems, so they should only be used for this purpose in the absence of a superior alternative such as HPE RM, a business information system or a wiki.

Problems with shared drives include:

• Lack of recordkeeping functionality, meaning that the authenticity and integrity of records cannot be established to the degree necessary to be able to rely upon the record as evidence.
• Lack the granularity of security permissions available in an EDRMS.
• Lack of sophisticated search and reporting tools.
• Ease with which records can be deleted, replaced or tampered with.
• Lack of an audit trail to identify who has accessed and/or modified a record.
• Lack of metadata necessary to prove the authenticity and integrity of the record, e.g. proving that it was created or sent at a certain time, or proving it hasn’t been tampered with.
• Folder structures are usually poorly organised, resulting in difficulty finding records and the proliferation of duplicates.
• Difficulty in determining which version of a record is the most current and in tracking the revision history of records.
• Potential for obsolete/superseded documents and forms to remain in circulation/use, risking confusion and poor decision-making made on the basis of out-dated information.

There are a number of steps and actions that can be taken to improve the recordkeeping characteristics of shared drives. The most important step is to arrange the folders into a logical controlled structure based on business functions and activities and to provide guidelines for staff on which folders they should save different records in.

Security permissions should be set to restrict access to folders containing sensitive documents to authorised staff members, and to limit the ability of users to delete or amend records. Be aware when setting folder permissions that settings which allow users to save documents to a folder will also allow them to delete documents in that folder. Staff should remember that electronic records stored on the shared drives are still State Records and must not be deleted without authorisation.

Folder structure

The folder structure must be logical, consistent and clear, so everyone knows where to save and look for information. We recommend using a structure based on the UTAS Business Classification Scheme, as doing so will make it much easier to dispose of records with the same retention period, avoiding the need to individually appraise every record in a given folder.

The ability to create new folders should be restricted, especially when it comes to top-level and mid-level folders. This is essential for the preservation of the controlled folder structure and the promotion of consistent filing. Folder creation permissions should be restricted to one or two staff members who will be responsible for creating folders and managing the folder structure.

• Give each folder a clear and meaningful title that accurately reflects the contents of the folder. Avoid the use of jargon and acronyms, as these may lose their meaning over time.
• Ensure that each folder’s title differentiates the folder from similar folders and sub-folders, so it is clear where information should be saved.
• Avoid titles based on the names of staff members or position titles, e.g. “Mary’s documents”.
• Limit repetition in the titles of folders and their sub-folders.
• Limit the number and depth of sub-folders, as an overly complicated folder structure may cause confusion and lead to the misfiling of documents.
• Avoid names of organisational units, as these can change in restructures etc.

Guidelines and procedures

Guidance and training should be provided to assist staff in determining which folder to save or search for a record in. A set of guidelines and procedures describing how the folder structure works and how to save and retrieve records should be drawn up and saved in a prominent location on the shared drive.

Topics should include:

• Which records should be stored in which folders
• How to export and/or save records and which formats to use
• Where to capture emails and which emails to capture
• Who can create new folders and how to request their creation
• Who can delete documents and records and when they should be deleted
• When to delete obsolete versions and when (and where) to retain them
• Housekeeping responsibilities and schedules
Housekeeping audits

Business areas should conduct regular audits of the shared drives to check for duplication, misfiled records, obsolete versions and old reference materials, and to check that the procedures have been followed. Auditing responsibilities and scheduling requirements should be assigned and listed in the procedures dealing with use of the shared drives.

Capturing records in read-only formats

The final version and significant drafts of records should be captured as records in a read-only format such as a PDF. Although this provides no real protection against deliberate tampering, it at least reduces the risk of accidental/innocent alterations undermining the reliability of records and/or removing important information from records.

Where possible, records classed as having permanent value should be saved in PDF/A-1b format in order to preserve their long-term accessibility. Unfortunately, the conversion process is often complicated by errors caused by complex technical issues, so this is not always viable.

Document properties

You should capture the following metadata for each document using the document properties:

- Title
- Author
- Version
- Publication date
- Company
- Related records
- Home folder

Note that system dates such as "Date Created" can be affected by system events such as moving the file, making them unreliable. Use "Publish Date" or a custom field instead.

To edit the document properties in Adobe Acrobat, select Properties from the File menu. The title and author fields are available on the Description tab, but you will have to create the other fields using the Custom tab. To create a custom field, enter the name of the field in the “name” box and the relevant data in the “value” box (e.g. “Date scanned” & “21/5/2011”) and click “Add”.

Document footers

Adding the document title and file path to the footer of documents (and document templates) will assist in the tracking of documents and make it easier to find the latest version. It is also good practice to include the version number and draft status.

Sharing documents and records

Instead of using email attachments, which can cause problems with duplication and version control, staff should provide links to the location on the shared drive where the relevant documents are stored so that colleagues can work on and from the same documents.

Where not to store electronic records

Hard disks, removable media (e.g. USB drives, CDs/DVDs & floppy disks), personal email folders and cloud-based services are not recordkeeping systems and must not be used to store records.

Records stored on your hard disk, on CD-ROMs or USB drives are not backed up and could be lost or fall into the wrong hands (if on a USB drive). These storage mediums also lack important recordkeeping functionalities that enhance authenticity, integrity and accessibility.
While cloud-based storage options such as *Dropbox* and *PebblePad* can be very useful when working on draft documents, they pose a number of risks when it comes to recordkeeping, especially if the data is stored overseas. For more information, see [State Records Guideline 17 – Managing the recordkeeping risks associated with cloud computing](#).

**Capturing emails**

Emails can either be exported as PDFs and saved in the appropriate folder on the shared drive or stored in a shared email account. Shared email accounts allow everyone in the team to access emails stored in the shared folders and they are regularly backed up by ITS. The folders in a shared email account should be set up to mirror the same folder structure used for the shared drive. To set up a shared email account, contact the Service Desk.

Email attachments should be saved to the appropriate folder in the shared drive, as they may become difficult to access via the email even if stored in a shared email account due to the auto-archiving functions built into some email applications such as Microsoft Outlook. If the attachment is the final version of a document or needs to be captured as a record, it should then be exported to a read-only format such as PDF/A.
Appraisal and disposal

How long do I need to keep records?

The short answer is that it depends on the record. While all records of University business activities are subject to the requirements of the Archives Act, some records are obviously more important than other records, so it should not come as a surprise to learn that important records such as policies and contracts need to be kept longer than records of short-term value.

Contrary to common misconception, there is no ‘seven year rule’. Some records have to be kept a lot longer than that, while others can and should be destroyed sooner for privacy reasons etc. For example, ephemeral records can be destroyed as soon as you no longer need them, while permanent records must be kept for 25 years and then transferred to the State Archives.

To determine how long you need to keep a given record, you will need to consult the disposal schedules approved for use by the University. The disposal schedules are available on the RMU website and are discussed in detail below, but the key point to remember is that the disposal schedules list the retention periods for different types of records.

Disposing of records

Disposal in a recordkeeping sense doesn’t necessarily mean destroying records but rather any action that removes the records from the University’s custody, including:

a) Destruction of the records;
b) Transfer of permanent records to the Tasmanian Archive & Heritage Office;
c) Transfer of the records to another organisation or individual.

Of these, destruction is likely to be the most common, followed by transfer to the TAHO, while the third option is likely to be a rare occurrence.

To determine whether you can destroy records or will need to transfer them to the TAHO, you will need to establish whether they are temporary records or permanent records by looking them up in the disposal schedules.

Temporary records can be destroyed via a Records Destruction Request form once their retention period has expired; permanent records must be kept for 25 years and then transferred to the State Archives following submission of an Application to Dispose of State Records.

Disposal schedules

Under the Archives Act 1983, the University may not dispose of records without the written approval of the State Archivist. However, you don’t actually need to ask the State Archivist every time you wish to destroy a record, because the State Archivist has already issued a number of documents known as disposal schedules authorising the disposal of certain classes of records after an associated period of time known as a retention period.

These retention periods vary according to the long-term value of the records described in the corresponding disposal class. Records of very low or short-term value can be destroyed as soon as they are no longer needed, while records of high or historical value must be kept for 25 years and then transferred to the State Archives. Most records fall somewhere in between, with a retention period between one to ten years.

Note that the disposal schedules only apply to records dating from 1960 or later; earlier records must be treated as unscheduled records.

Disposal schedules applicable to the University

The University uses the four generic disposal schedules published by the Tasmanian Archive and Heritage Office (TAHO) along with its own approved functional disposal schedule (DA 2398) based on the specific business functions of the University. DA 2398 replaces the previous functional disposal schedule DS 32, which has been rescinded and is no longer valid.
The disposal schedules currently authorised for use at the University are:

- DA 2135 – Registered Training Organisations
- DA 2157 – Common Administrative Functions
- DA 2158 – Short-Term-Value Records
- DA 2159 – Temporary Value Source Records
- DA 2398 – UTAS Functional Disposal Schedule

**Disposal classes**

Each disposal schedule is made up of a number of disposal classes, organised by business function and activity. Each disposal class describes a class of records (e.g. invoices) and has a corresponding reference number and a disposal action, identifying whether those records are temporary or permanent records, and listing their retention period (if temporary).

To locate the appropriate disposal class for a given folder or collection of records, start by identifying the appropriate disposal schedule and read through the descriptions provided for each function to identify which function would be most relevant to the records in question.

Each function will have a number of activity subheadings listed under it: select the most applicable, then look through the disposal classes listed under that activity to see if you can find one that describes the records.

If you can’t find a suitable disposal class, try looking under another function or activity, checking the index (if there is one) or searching the PDF for keywords. If you still can’t find anything suitable, they may be unscheduled. Please resist the temptation to ‘squeeze’ records into a disposal class that would require a strained reading of the class description, and remember that you cannot use a function or activity heading in place of a disposal class. If in doubt, ask the RMU for advice.

**Unscheduled records**

Unscheduled records are records that do not fit into any of the disposal classes listed in the disposal schedules applicable to the University, usually because they represent classes of records unique to the University that currently fall into one of the gaps in the University’s functional disposal schedule (DA 2398). If you do come across any records you believe may be unscheduled, please contact the Records Management Unit. We may be able to suggest a class you have overlooked, or failing that, ensure that the gap is addressed the next time the disposal schedule is reviewed.

To dispose of unscheduled records, you will need to describe them in an Application to Dispose of State Records and submit it to the Tasmanian Archive & Heritage Office (TAHO). In most cases, you will be asking for permission to destroy the records, but if you believe they may have sufficient historic or cultural value to warrant permanent retention, you may instead recommend that the records are transferred to the State Archives.

If you wish to destroy any or all of the records listed in the Application to Dispose of State Records, you will need to complete the TAHO’s Destruction Authority checklist and submit it along with the Application. If approved, the TAHO will issue you with a Destruction Authority for the records - you must not destroy the records until you have received this. Records should be destroyed using a secure and confidential process appropriate to the record format. You do not need to list records authorised for destruction under a Destruction Authority in a Register of Records Destroyed.
Destroying records

It is against the law to destroy University records without the State Archivist's authorisation. Some high-value records known as permanent records must never be destroyed, but the vast majority of records are temporary or ephemeral records, whose destruction has been authorised by the State Archivist upon expiration of the retention period assigned to their disposal class.

In the case of ephemeral records, this is as soon as they are no longer needed, and these records can be freely destroyed without further authorisation.

However, before destroying any temporary records, they must be listed in a Records Destruction Request form along with the reference numbers of the disposal classes authorising their destruction and the date range of the records. These forms provide evidence that the destruction of the records was authorised and must be approved by the Records Management Unit before the records can be destroyed.

Once the Records Destruction Request has been approved, the records must be securely destroyed via a destruction method appropriate to their format, e.g. a locked shredding bin. Contact the Records Management Unit for advice on appropriate destruction methods for records stored in unusual formats.

The destruction of non-ephemeral records must be recorded in a Register of Records Destroyed for the business unit, describing the records that were destroyed and the dates they were destroyed. This must be signed off by the head of the business area on an annual basis.

Destruction holds

There are some special circumstances under which records may be subject to a temporary destruction hold, during which you may not destroy them even if their retention period has expired. Destruction holds may apply to records that relate to imminent, likely or ongoing...

- legal action, both civil and criminal
- government investigations and inquiries
- Native Title claims and
- Right to Information requests.

Records relating to indigenous families and communities or which document links between indigenous people and localities are also subject to special restrictions and should be the subject of consultation with the TAHO.

In most cases, destruction holds will be issued by the Legal Office or the Records Management Unit, who will advise you which records are subject to the hold and when the hold has been lifted. If you are not sure whether any of these circumstances would apply to records in your possession, please contact the Records Management Unit for advice.

Records Destruction Requests

The Records Destruction Request (RDQ) form can be downloaded from the RMU website. It takes the form of an Excel spreadsheet template and is designed to be filled out and submitted in Excel format, as this makes it easier to read and amend if necessary before it is approved by the RMU.

Type your business unit's name in the space provided. Fill in a row for each group of records belonging to the same disposal class. You don't need to create a separate entry for each folder unless they relate to different projects or the description is too complex to fit on one line. You must complete all the columns for each entry for the register to be valid. Please don't use "ditto" marks.

Enter an accurate description of the records that will be meaningful to people outside your business unit. The Records Management Unit needs to be able to determine the nature of the records from the description field and accurately assess whether they would be covered by the nominated disposal class. With the exception of "UTAS" and unit codes, avoid acronyms and abbreviations. If you must use acronyms, the first instance should be listed in full followed by the acronym in brackets, e.g. "Australian Maritime College (AMC)".
Enter the date range of the records described, from the date of the oldest record to the date of the newest record. Try to be as specific as possible, but month and year is generally sufficient, e.g. Feb 2001. If the records are undated, please provide a conservative circa date (prefixed with "c."), e.g. "these must have been created in 2005 at the latest, because that was when we stopped offering this course, so I'll list the end date as c. 2005". Please check the end date for each entry and ensure that the retention period has expired.

Submission process

1. Download the form from the RMU website.
2. Please fill out the form in Excel, starting with the name of your business unit.
3. List the records you wish to destroy along with the disposal classes you are citing as authorisation and the start and end dates of the folder.
4. Email the draft to the RMU for approval in Excel format. The RMU will reply, either approving the destruction or asking you to clarify and/or amend any problematic entries or details.
5. Once you receive approval to destroy the records from the RMU, destroy the records securely and confidentially (e.g. using a secure shredding bin).
6. Certify that the records have been destroyed by listing their details and the destruction date in your business area’s Register of Records Destroyed. You can copy and paste the entries from the Records Destruction Request into the Register of Records Destroyed.

Tips for avoiding a resubmission request

- Remember to include your business area’s name.
- Ensure descriptions are meaningful. Don’t use acronyms or abbreviations.
- You can’t use reference numbers ending “.00” (these indicate headings).
- Make sure you fill in all the columns for each entry/row.
- Double-check the dates against the retention periods to make sure they have actually expired. Pay careful attention to when the period actually starts.
- Don’t list ephemeral records (e.g. anything that falls under DA 2158).

Registers of Records Destroyed

All University business areas are required to create Registers of Records Destroyed (RRDs) to register when records are destroyed and verify that their destruction was authorised under an approved disposal schedule. A separate Register of Records Destroyed should be created for each year.

Registers of Records Destroyed are central to the accountability process built into the disposal schedules and must be signed off on by the head of the organisational unit responsible for the records at the end of the year.

It is important to recognise that Registers of Records Destroyed are the formal evidential records of the destruction process and are periodically audited by the State Archivist. Copies of completed registers must be sent to the RMU so they can be forwarded to the State Archivist upon request.

Registers should not be used to list unscheduled records as these will be covered by a Destruction Authority issued by the State Archivist. Nor is it necessary to make entries for records destroyed under the authority of DA 2158 or DA 2159, as it is expected that these low value records will be destroyed on a routine basis. Permanent records must not be destroyed and should therefore never be listed on a Register of Records Destroyed.

TAHO audit

The Tasmanian Archive & Heritage Office periodically audits the University's recordkeeping practices, including examining Registers of Records Destroyed to check whether they have been filled out correctly and ensure the destruction of any records has been authorised under an appropriate disposal class.

As Registers of Records Destroyed must be made available to the TAHO upon request, copies of completed registers should be forwarded to the RMU at the end of the year when they are signed off by the head of the business area.
Transferring records to the TAHO

To transfer permanent records to the TAHO, you will need to list the records and their disposal classes in an Application to Dispose of State Records and submit it to the TAHO. List records in the order in which they were maintained when they were active, whether that is chronological, alphabetical or some other arrangement. If there is no obvious ordering system, leave the records in the order they were found in.

You can also apply to transfer any unscheduled records you believe may have permanent value via the same method, though in this case you will need to indicate that the records are unscheduled instead of citing a disposal class. If you need help or advice, contact the Records Management Unit for assistance.

Preparing permanent records for transfer

Before transferring the records, you will need to prepare them by removing any staples or metal paperclips, as these can leave rust marks. For similar reasons, records housed in lever arch folders or metal ring binders should be transferred to archival folders with plastic tube clips. If the original folder was labelled, this information must be transferred to the replacement folder.

Plastic dividers and sleeves (e.g. those found in 'display folders') often contain plasticisers which can cause rapid deterioration in paper records within a few years, so all plastic should be removed and replaced with cardboard dividers.

The adhesive in sticky notes can also damage records over time, so remove and replace any important notes with photocopies. Records printed on thermal paper such as faxes and receipts should be replaced with photocopies.

If the records are dirty, you will need to carefully remove any loose dirt and debris before they can be transferred. It is especially important to make sure that there is no mould present; if you do find any mould, please contact the Records Management Unit immediately, as mould spreads quickly and can cause severe damage to paper records, so it must be treated as soon as possible.

Setting access restrictions

Permanent records will eventually be added to the state archives and open to the general public, so it is important to consider whether the records contain any sensitive information that would warrant restricting access for a time. As permanent records are normally only transferred after 25 years, some information will have long since ceased to be sensitive while other records will never have contained sensitive information, but some may need to be protected for longer.

You can apply to restrict access to records for 50 years or 75 years, and can also specify who should be allowed to access it during that time, including giving the State Archivist discretion to allow researchers etc. access on case by case basis.

Some factors to consider include whether the record:

- Contains information that was communicated in confidence
- Contains sensitive personal information about individuals
- Contains information likely to prejudice pending or likely legal proceedings

For more information, see State Recordkeeping Guideline 4: Agency Determination of Access Restrictions.

For more information, see State Recordkeeping Advice 12: Preparing records for transfer.
## Appendices

### Appendix A: Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audit Trail</strong></td>
<td>Data that allows the reconstruction of a previous activity, or which enables attributes of a change (such as date, time or operator) to be stored so that a sequence of events can be determined in the correct chronological order. It is usually in the form of a database or one or more lists of activity data.</td>
</tr>
<tr>
<td><strong>Appraisal</strong></td>
<td>The process of evaluating records to determine which are to be retained as archives, which are to be kept for specified periods and which will be destroyed.</td>
</tr>
</tbody>
</table>
| **Archives**       | 1. Records that are appraised as having archival value. This definition of the term differs from that used in the IT sphere where it refers to a copy of one or more files, or a copy of a database that is saved for future reference or for recovery purposes in case the original data is damaged or lost.  
2. A place such as a building, room or storage area where archival material is kept.  
3. An organisation (or part of an organisation) responsible for appraising, acquiring, preserving and making available archival material. E.g. Tasmanian Archive and Heritage Office. |
| **Born Digital**   | Any media or records which have been generated entirely electronically, e.g. a document created in a word processing application, as opposed to a scanned image of a paper document. |
| **Business Activity** | An umbrella term covering all the functions, activities and transactions of an organisation and its employees. Business activity is used as a broad term, not restricted to commercial activity and including public administration, non-profit and other activities. |
| **Business Function** | The first level of a business classification scheme. Functions represent the major responsibilities that are managed by the organisation to fulfil its goals. They are high-level aggregates of the organisation’s activities. |
| **Business Classification Scheme (BCS)** | A conceptual representation of the functions and activities performed by an organisation. The scheme is derived from the analysis of business activity. It is the basis from which classification tools, such as a functions thesaurus and record classification scheme, are developed. These tools help agency personnel create meaningful titles for records. |
| **Business Information System (BIS)** | An automated system that creates or manages information about an organisation’s activities. Includes applications whose primary purpose is to facilitate transactions between an organisational unit and its customers e.g. an e-commerce system, client relationship management system, purpose-built or customised database, finance or human resources systems. Business information systems that create or manage records should have the appropriate functionally for these tasks, or they should interface with other systems that manage the records. |
| **Business Unit**  | Refer to Organisational Unit (OU)                                                                                                                                                                         |
**Capture**
The process of lodging a document or digital object into a recordkeeping system and assigning metadata to describe the record and place it in context, thus allowing the appropriate management of the record over time. For certain business activities this functionality may be built into business information systems so that the capture of records is concurrent with the creation of records.
See also Registration.

**Caveat**
A non-hierarchical qualifier (such as commercial-in-confidence) attached to a security category to limit access to particular records. Caveats are implemented as active metadata by applying access controls or defining special record types.

**Classification**
1. The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system.
2. Determining document or file naming conventions, user permissions and security restrictions on records.

**Continuum**
The whole extent of a record's existence. The related theory replaces the life cycle model by considering that records require management starting before they are created, e.g. in systems design. This theoretical model more effectively allows for preservation and management processes to be applied to a record at any point in time, which is particularly relevant when dealing with digital records.

**Copyright**
The exclusive right, granted by law, of the creator of a work (or his/her assignees or employers) to make or dispose of copies and otherwise control the use of a literary, dramatic, musical, artistic or other work. Ownership of copyright in a work does not necessarily pass with ownership of the work itself. The laws relating to copyright are complex and require specialist legal advice.

**Create (a record)**
To make a record (evidence) of business transactions.

**Custody**
The responsibility for the care of records and archives, usually based on their physical possession. Custody does not necessarily include legal ownership.

**Data**
Facts or instructions represented in a formalised manner, suitable for transmission, interpretation or processing manually or automatically.
See also Metadata

**Database**
An organised collection of related data. Databases are usually structures and indexed to improve user access and retrieval of information. They may exist in physical or digital format.
<table>
<thead>
<tr>
<th>Deletion</th>
<th>The process of removing, erasing or obliterating recorded information from a medium outside the disposal process. Deletion within electronic systems generally refers to the removal of the pointer (i.e. location information) that allows the system to identify where a particular piece of data is stored on the medium. Deletion does not meet the requirements for destruction of Commonwealth records as it may be possible to retrieve the deleted data before it is completely over-written and obliterated by the system.</th>
</tr>
</thead>
</table>
| Destruction | 1. The process of eliminating or deleting records beyond any possible reconstruction.  
2. The Tasmanian Archive and Heritage Office authorises the disposal of State Records (including destruction) for the purposes of the Archives Act 1983. Destruction should be carried out by an approved method such as shredding or, in the case of electronic records, rendering them unreadable. |
| Digital Signature | A security mechanism included within a digital record that enables the identification of the creator of the digital object and can also be used to detect and track any changes that have been made to the digital object. Also known as an electronic signature. A scanned signature is not a digital signature. |
| Disposal | The range of processes associated with implementing records retention, destruction or transfer decisions which are documented in retention and disposal schedules or other instruments |
| Disposal Action | An action stipulated in a Retention & Disposal Schedule indicating the minimum retention period for a record and the event in relation to which the disposal date should be calculated.  
See also Disposal Trigger |
| Disposal Class | 1. The descriptor of a group of records which document similar activities. The disposal class includes a disposal action to be applied to the group in addition to function and activity terms, a scope note, a record description and a unique class number.  
2. A component of a records authority which acts as a set of rules within an electronic records management system. It is comprised of a disposal trigger, a retention period and a disposal action which may be applied to a record plan entity. |
<p>| Disposal Schedule | See Retention and Disposal Schedule. |
| Disposal Trigger | The point from which the disposal action is calculated. This can be a date on which action is completed or a date on which an event occurs. Examples include ‘Destroy 20 years after last action’ or ‘Destroy 75 years after date of birth’. See also Disposal Action and Retention Period. |
| Document | Recorded information or an object that can be treated as a unit. |</p>
<table>
<thead>
<tr>
<th><strong>Electronic Record</strong></th>
<th>A record created, communicated and/or maintained by means of electronic equipment. Although this term can refer to analogue materials (e.g. videotapes), it generally refers to records held in digital form on magnetic or optical computer storage media.</th>
</tr>
</thead>
</table>
| **File**             | 1. An organised unit of documents accumulated during current use and kept together because they deal with the same subject, activity or transaction.  
2. The action of placing documents in a predetermined location according to a scheme of control. |
| **Folder**           | An aggregation of records allocated to a records category within the records classification scheme. A folder is constituted of metadata that may be inherited from the parent (records category) and passed on to a child (record). |
| **Inactive Record**  | A record that is not required to be readily available for the business purposes of a department or agency and may therefore be transferred to intermediate storage, archival custody or be destroyed subject to applicable laws. |
| **Indexing**         | The process of establishing access points to facilitate retrieval of records and/or information. |
| **Information**      | Any type of knowledge that can be exchanged. In an exchange, it is represented by data. An example is a string of bits (the data) accompanied by a description of how to interpret a string of bits as numbers representing temperature observations measured in degrees Celsius (the representation information). |
| **Metadata**         | Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time. Metadata is attached to records when they are created and added to as a result of different processes such as sentencing and disposal.  
See also Data |
| **Migration**        | The act of moving records from one system to another while maintaining their authenticity, integrity, reliability and usability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another. |
| **Off-site storage** | A general term describing location arrangements for records. The storage might be leased by the university or held by a storage provider. The university contracts the storage provider to care for the records on their behalf. |
| **Organisational Unit (OU)** | Faculty, School, Centre, University Institute, other University Entity, Division, Section or University Business Enterprise. See Business Unit. |
| **Permanent Records**| Permanent records are records that are deemed to have long-term value even after their immediate value as evidence of business activities has elapsed, usually for their potential historical/cultural value. |
| **Preservation** | The processes and operations involved in ensuring the technical and intellectual survival of authentic records through time. Preservation encompasses environmental control, security, creation, storage, handling, and disaster planning for records in all formats, including digital records. |
| **Records** | Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.  
See University Records |
| **Record Type** | The definition of a record object that specifies particular management requirements, metadata attributes and forms of behaviour. A default record type is the norm. Specific record types are deviations from the norm, which allow an organisation to meet regulatory requirements (such as privacy or data matching) for particular groups of records. |
| **Recordkeeping** | The making and maintaining of complete, accurate and reliable evidence of business transactions in the form of recorded information. Recordkeeping includes the creation of records in the course of business activity, the means to ensure the creation of adequate records, the design, establishment and operation of recordkeeping systems and the management of records used in business (traditionally regarded as the domain of records management) and as archives (traditionally regarded as the domain of archives administration). |
| **Recordkeeping System** | A framework to capture, maintain and provide access to evidence of transactions over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices. Recordkeeping systems include:  
- both records practitioners and records users  
- a set of authorised policies, assigned responsibilities, delegations of authority, procedures and practices  
- policy statements, procedures, user guidelines and other documents that are used to authorise and promulgate the policies, procedures and practices  
- the records themselves  
- specialised information and records systems used to control the records  
- software, hardware, other equipment and stationery. |
| **Records Management** | The field of management responsible for 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. |
| **Registration** | The act of giving a record or file a unique identity in a recordkeeping system to provide evidence that it was created or captured. Registration involves recording brief descriptive information about the context of the record and its relation to other records. In the archival context, both aggregations (such as series) and individual record items can be registered. See also Capture. |
| **Repository** | The building or room, or part thereof, set aside for storing records. Archival repositories are often constructed to meet specific environmental standards designed to ensure the longevity of the records. |
| **Retention and Disposal Schedule** | Retention and Disposal Schedules (sometimes called Disposal Authorities or simply Disposal Schedules) identify business functions and activities, describe the types of records associated with each function/activity pair, and prescribe a disposal action. These schedules are legal documents that provide the necessary authorisation by the State Archivist to allow disposal to be undertaken. Disposal actions range from permanent retention as an archive, to stipulating a minimum period of retention prior to destruction. |
| **Retention Period** | The length of time after the disposal trigger that a record must be maintained and accessible. At the expiration of the retention period, a record may be subject to disposal. See also Disposal Trigger |
| **Sentencing** | The process of identifying the disposal class a record belongs to and applying the disposal action specified in the relevant disposal schedule. Sentencing is the implementation of decisions made during appraisal. |
| **Source Record** | A document or record that has been copied, converted or migrated or will be the input for such a process. A source record may be an original record or it may be a reproduction that was generated by an earlier copying, conversion or migration process. |
| **Structured Data** | A record created from data that has been collated and managed in a structured environment, often in a database-type business information system. The captured data is highly-structured, predictive and repetitive. |
| **Temporary record** | A record that has value for a finite period of time only to the Australian community, the individuals and organisations that do business with the State and State Government agencies and statutory authorities themselves. Temporary records are needed by agencies to meet specific accountability requirements. |
| **Transaction** | 1. The smallest unit of a business activity. 2. The third level in a business classification scheme. 3. The process of a request being made on a website and a service being received and/or acknowledgement of the request. |
| **HPE RM** | HPE Records Manager (HPE RM) is the University's Electronic Document and Records Management System (EDRMS). It manages electronic and hard copy records, enabling saving, editing, locating, tracking, archiving and disposal of information in the one system. |
### University Employee

Any individual employed by the University of Tasmania, including permanent, fixed-term and casual staff members and any contractors or consultants hired to perform work on behalf of the University.

### University Records

University records are records relating to the business activities of the University of Tasmania. The University owns all records created and received by individual employees as part of their day to day business, including research data, teaching materials and correspondence. Under the Archives Act 1983, the University's records are State Records and must be managed and disposed of in accordance with the Act.

See Records

### Unscheduled Records

Unscheduled records are University records that are not described in any of the disposal classes listed in current Retention and Disposal Schedules. Lacking a disposal class to cite, authorisation to dispose of unscheduled records can be sought directly from the State Archivist by submitting an Application to Dispose of State Records.

### Vital records

The records without which an organisation could not continue to operate, i.e. those containing information needed to re-establish the organisation in the event of a disaster. Vital records are those that protect the assets and interests of the organisation as well as those of its clients and shareholders.
Appendix B: Key disposal classes

The following disposal classes are among the most frequently used at UTAS and are listed here for ease of reference. Please note that this is not a complete list and must be used in conjunction with the disposal schedules, not instead of them. If you are not sure whether a record falls within one of the classes listed here, please consult the full entry in the relevant disposal schedule and/or seek advice from the RMU, rather than try to squeeze it into a class that may not be appropriate.

<table>
<thead>
<tr>
<th>Disposal Schedule</th>
<th>Disposal Class</th>
<th>Short Description</th>
<th>Disposal Action / Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA 2157 05.01.01</td>
<td></td>
<td>Invoices and receipts</td>
<td>Destroy 7 years after action completed</td>
</tr>
<tr>
<td>DA 2157 05.01.04</td>
<td></td>
<td>Banking records and credit card statements</td>
<td>Destroy 7 years after action completed</td>
</tr>
<tr>
<td>DA 2157 05.01.11</td>
<td></td>
<td>Inter-Departmental Requisitions</td>
<td>Destroy 7 years after action completed</td>
</tr>
<tr>
<td>DA 2157 05.07.01</td>
<td></td>
<td>Budgeting records</td>
<td>Destroy 7 years after action completed</td>
</tr>
<tr>
<td>DA 2157 06.04.01</td>
<td></td>
<td>Vehicle requisition forms/books</td>
<td>Destroy 2 years after action completed</td>
</tr>
<tr>
<td>DA 2157 09.11.02</td>
<td></td>
<td>Registers of Records Destroyed</td>
<td>PERMANENT – transfer after 25 years</td>
</tr>
<tr>
<td>DA 2157 12.03.01</td>
<td></td>
<td>International and domestic travel approval forms</td>
<td>Destroy 2 years after action completed</td>
</tr>
<tr>
<td>DA 2157 12.11.04</td>
<td></td>
<td>Time sheets and Time-Off-In-Lieu (TOIL) sheets</td>
<td>Destroy 3 years after completion of the annual audit</td>
</tr>
<tr>
<td>DA 2157 12.16.01</td>
<td></td>
<td>Applications for leave and supporting documentation</td>
<td>Destroy 3 years after action completed (including checking)</td>
</tr>
<tr>
<td>DA 2157 12.18.02</td>
<td></td>
<td>Performance management evaluations</td>
<td>Destroy 2 years after action completed</td>
</tr>
<tr>
<td>DA 2157 14.12.01</td>
<td></td>
<td>Master copies of all significant University publications</td>
<td>PERMANENT – transfer after 25 years</td>
</tr>
<tr>
<td>DA 2157 15.13.01</td>
<td></td>
<td>Content, attendance and financing of internal training programs</td>
<td>Destroy 7 years after action completed</td>
</tr>
<tr>
<td>DA 2157 15.13.02</td>
<td></td>
<td>Administrative arrangements for training programs</td>
<td>Destroy 2 years after course completed</td>
</tr>
<tr>
<td>DA 2157 16.12.01</td>
<td></td>
<td>Non-committee meetings pertaining to the overall management of the unit/section</td>
<td>Destroy 2 years after action completed</td>
</tr>
<tr>
<td>DA</td>
<td>Date</td>
<td>Description</td>
<td>Retention</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>DA</td>
<td>02.13.07</td>
<td>Exam scripts (completed answer booklets/papers)</td>
<td>Destroy 1 year after relevant examination period</td>
</tr>
<tr>
<td>DA</td>
<td>06.03.02</td>
<td>Uncollected student assignments, essays and tests</td>
<td>Destroy after completion of assessment results</td>
</tr>
<tr>
<td>DA</td>
<td>06.10.02</td>
<td>Student Evaluation of Teaching &amp; Learning (SETL) questionnaires</td>
<td>Destroy 1 year after action completed</td>
</tr>
<tr>
<td>DA</td>
<td>06.21.01</td>
<td>Master copies of unit outlines</td>
<td>Destroy 10 years after the unit is signed-off by the school</td>
</tr>
<tr>
<td>DA</td>
<td>06.21.02</td>
<td>Unit materials and lecture recordings</td>
<td>Destroy 3 years after action completed</td>
</tr>
<tr>
<td>DA</td>
<td>06.21.04</td>
<td>Student placements/practicums</td>
<td>Destroy 2 years (if the result has been entered into the student information system) or 10 years after action completed</td>
</tr>
<tr>
<td>DA</td>
<td>12.06.01</td>
<td>Key University committees</td>
<td>PERMANENT – transfer after 25 years</td>
</tr>
<tr>
<td>DA</td>
<td>19.18.02</td>
<td>Successful applications for research grants</td>
<td>Destroy 7 years after action completed</td>
</tr>
<tr>
<td>DA</td>
<td>19.18.03</td>
<td>Unsuccessful applications for research grants</td>
<td>Destroy 3 years after action completed</td>
</tr>
</tbody>
</table>
Appendix C: Disposal Flow Chart

1. **Sort records into groups of similar records for processing.**
2. **Are the records covered by DA 2158 (Short-term-value records)?**
   - Yes: **Destroy when reference ceases. Do NOT list in a Register of Records Destroyed.**
   - No: **Check other schedules: DA 2398, DA 2157, DA 2159, and DA 2135.**
3. **Determine the most appropriate function and activity.**
4. **Is there a suitable disposal class there?**
   - Yes: **Add to Register of Inactive Records and retain for 25 years, then transfer them to State Archives using an Application to Dispose of State Records.**
   - No: **Check the disposal action: is the status PERMANENT?**
     - Yes: **Contact the Records Management Unit for further advice.**
     - No: **Has the retention period expired?**
       - Yes: **The records are unscheduled - submit an Application to Dispose of State Records.**
       - No: **Do the records relate to:***
         - an inquiry or investigation?
         - imminent legal action?
         - a Right to Information request?
         - a Native Title claim?
         - indigenous communities or sites?
         - If yes, then **List records in a Records Destruction Request form with the reference number of the disposal class and submit it to the Records Management Unit for approval.**
         - If no, then **Try the index and a keyword search of the PDF: did you find a suitable disposal class?**
           - Yes: **The records are unscheduled - submit an Application to Dispose of State Records.**
           - No: **Add to Register of Inactive Records and retain until retention period expires.**
2. **Upon approval, destroy the records and list the records destroyed in your area's Register of Records Destroyed for the current year, along with the applicable RDA ID and the date the records were destroyed.**
3. **At the end of the year, have the Register of Records Destroyed signed off by the head of your business area and send a copy to the Records Management Unit.**