Contents

1 Executive Summary ................................................................. 4
2 More information .................................................................. 4
3 Legislative obligations .......................................................... 4
3.1 Identifying recordkeeping requirements ............................... 5
3.2 What is a record? ............................................................... 6
3.3 When does a document become a record? ......................... 6
3.4 Determining which information to capture ......................... 6
3.5 When to capture a record .................................................... 7
3.6 When to create a record ...................................................... 7
4 Types of records .................................................................... 8
4.1 University records ............................................................. 8
4.2 Vital records ...................................................................... 8
4.2.1 Vital Records Register .................................................. 9
4.3 Permanent records ............................................................ 9
4.4 Temporary records ............................................................ 10
4.5 Ephemeral (short-term value) records ................................. 10
4.6 Personal records .............................................................. 11
4.7 Active Records ............................................................... 11
4.8 Inactive Records ............................................................. 11
5 Record formats ..................................................................... 11
5.1 Electronic records ............................................................ 11
5.1.1 Email records .............................................................. 12
5.1.2 Web sites .................................................................. 12
5.1.3 Social media and Cloud hosted services ....................... 13
5.1.4 Distribution and publication of electronic records ....... 14
5.2 Paper records .................................................................. 14
5.2.1 Facsimile transmissions .............................................. 14
5.3 Source records ............................................................... 14
5.3.1 Reproduction conditions for digitising source records .... 15
5.4 Publications .................................................................... 15
6 Managing records ................................................................. 16
6.1 Who owns University records? ........................................ 16
6.2 Who manages University records? .................................... 16
6.3 Folders ........................................................................... 16
6.3.1 Physical folders .......................................................... 16
6.3.2 Electronic folders ......................................................... 17
6.4 Transfer of University records to other organisations/institutions ........................................... 17
6.5 Outsourcing – Recordkeeping issues .................................. 17
6.6 Privatisation – Recordkeeping issues ................................. 18
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Recordkeeping Systems</td>
<td>18</td>
</tr>
<tr>
<td>7.1</td>
<td>What is a recordkeeping system?</td>
<td>18</td>
</tr>
<tr>
<td>7.2</td>
<td>What is recordkeeping metadata?</td>
<td>19</td>
</tr>
<tr>
<td>7.3</td>
<td>What is a classification scheme?</td>
<td>19</td>
</tr>
<tr>
<td>7.4</td>
<td>What is the disposition of a record?</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>Access and security of records</td>
<td>20</td>
</tr>
<tr>
<td>8.1</td>
<td>Folders and documents</td>
<td>21</td>
</tr>
<tr>
<td>8.2</td>
<td>University archived records held by the Tasmanian Archive and Heritage Office</td>
<td>21</td>
</tr>
<tr>
<td>8.3</td>
<td>Breaches of access and/or security</td>
<td>22</td>
</tr>
<tr>
<td>9</td>
<td>Storage of Records</td>
<td>22</td>
</tr>
<tr>
<td>9.1</td>
<td>Storage of Confidential and Sensitive records</td>
<td>22</td>
</tr>
<tr>
<td>9.2</td>
<td>Physical storage</td>
<td>23</td>
</tr>
<tr>
<td>9.3</td>
<td>Electronic storage</td>
<td>23</td>
</tr>
<tr>
<td>9.4</td>
<td>Using shared folders in conjunction with a recordkeeping system</td>
<td>24</td>
</tr>
<tr>
<td>9.5</td>
<td>Off-site storage of inactive records</td>
<td>25</td>
</tr>
<tr>
<td>9.6</td>
<td>Storing records in the Cloud</td>
<td>26</td>
</tr>
<tr>
<td>10</td>
<td>Preservation/protection of records</td>
<td>26</td>
</tr>
<tr>
<td>10.1</td>
<td>Physical Records</td>
<td>27</td>
</tr>
<tr>
<td>10.2</td>
<td>Digital formats</td>
<td>27</td>
</tr>
<tr>
<td>11</td>
<td>Disposal of records</td>
<td>28</td>
</tr>
<tr>
<td>11.1</td>
<td>Records Disposal Program</td>
<td>28</td>
</tr>
<tr>
<td>11.2</td>
<td>Appraisal of records</td>
<td>29</td>
</tr>
<tr>
<td>11.3</td>
<td>Disposal authorisation</td>
<td>29</td>
</tr>
<tr>
<td>11.4</td>
<td>Retention and Disposal Schedules</td>
<td>30</td>
</tr>
<tr>
<td>11.5</td>
<td>Unscheduled records</td>
<td>30</td>
</tr>
<tr>
<td>11.6</td>
<td>Destruction</td>
<td>30</td>
</tr>
<tr>
<td>11.6.1</td>
<td>Records Destruction Requests</td>
<td>31</td>
</tr>
<tr>
<td>11.6.2</td>
<td>Registers of Records Destroyed</td>
<td>31</td>
</tr>
<tr>
<td>11.6.3</td>
<td>Destroying paper records</td>
<td>31</td>
</tr>
<tr>
<td>11.6.4</td>
<td>Destroying electronic records</td>
<td>32</td>
</tr>
<tr>
<td>11.7</td>
<td>Transfer</td>
<td>32</td>
</tr>
<tr>
<td>11.7.1</td>
<td>Permanent records</td>
<td>32</td>
</tr>
<tr>
<td>11.7.2</td>
<td>Temporary records</td>
<td>32</td>
</tr>
<tr>
<td>11.7.3</td>
<td>Records copied into other media</td>
<td>32</td>
</tr>
<tr>
<td>12</td>
<td>Tasmanian Archive and Heritage Office (TAHO)</td>
<td>33</td>
</tr>
<tr>
<td>12.1</td>
<td>Transfer of records to the Tasmanian Archive and Heritage Office (TAHO)</td>
<td>33</td>
</tr>
<tr>
<td>12.2</td>
<td>Access requirements for state records</td>
<td>34</td>
</tr>
<tr>
<td>13</td>
<td>Right to Information</td>
<td>34</td>
</tr>
<tr>
<td>13.1</td>
<td>Disposal of records with regard to the Right to Information Act 2009</td>
<td>35</td>
</tr>
<tr>
<td>13.2</td>
<td>Retention of records for Right to Information purposes</td>
<td>35</td>
</tr>
<tr>
<td>13.3</td>
<td>Access to archived records for Right to Information purposes</td>
<td>35</td>
</tr>
<tr>
<td>14</td>
<td>Privacy</td>
<td>35</td>
</tr>
<tr>
<td>15</td>
<td>Responsibilities</td>
<td>35</td>
</tr>
<tr>
<td>16</td>
<td>Glossary</td>
<td>37</td>
</tr>
<tr>
<td>17</td>
<td>Versioning</td>
<td>43</td>
</tr>
<tr>
<td>18</td>
<td>Appendix 1 – Legislative obligations</td>
<td>44</td>
</tr>
<tr>
<td>18.1</td>
<td>University of Tasmania Act 1992</td>
<td>44</td>
</tr>
<tr>
<td>18.2</td>
<td>Archives Act 1983 &amp; Archives Regulations 2004</td>
<td>44</td>
</tr>
<tr>
<td>18.2.1</td>
<td>Section 10 - Preservation of State Records</td>
<td>44</td>
</tr>
<tr>
<td>18.2.2</td>
<td>Section 10A - State Archivist may issue guidelines</td>
<td>45</td>
</tr>
<tr>
<td>18.2.3</td>
<td>Section 20 - Disposal, destruction, &amp;c., of State records</td>
<td>45</td>
</tr>
<tr>
<td>18.3</td>
<td>Electronic Transactions Act 2000</td>
<td>45</td>
</tr>
<tr>
<td>18.4</td>
<td>Evidence Act 2001</td>
<td>46</td>
</tr>
<tr>
<td>18.5</td>
<td>Financial Management and Audit Act 1990</td>
<td>46</td>
</tr>
<tr>
<td>18.6</td>
<td>Financial Management and Audit Regulations 2003</td>
<td>46</td>
</tr>
</tbody>
</table>
18.7 Limitation Act 1974 ................................................................. 46
18.8 Personal Information Protection Act 2004 .................................. 46
18.9 Right to Information Act 2009 .................................................. 47
18.9.1 Section 11 – Information held by Archives Office ...................... 47
18.10 Work Health and Safety Act 2012 and Work Health & Safety Regulations 2012 .... 48
19 Appendix II - Recommended storage media for physical/paper records .............. 49

Responsible Officer

Jeff Murray, Chief Information Officer

Approved by

Jeff Murray, Chief Information Officer

Approved and commenced

(January 2018)

Review by

May, 2020

Relevant Policy or Procedure the Guideline supports

Records Management Policy

Responsible Organisational Unit

Records Management Unit
1 Executive Summary

These Guidelines outline the University’s recordkeeping requirements to support its business, legal and regulatory obligations and are applicable to all University employees, including contractors, consultants and University entities. These Guidelines aim to:

- inform employees of their responsibilities in relation to recordkeeping requirements
- assist in the development of procedures and business practices to support recordkeeping requirements
- assist compliance to business, legal and regulatory recordkeeping requirements.

These Guidelines should be used in conjunction with other resources available to support recordkeeping requirements including: information sheets, advices, templates, workshops, online learning modules, disposal schedules, classification schemes and recordkeeping systems.

2 More information

For further information, contact the Records Management Unit:

Email: RMU.Staff@utas.edu.au

3 Legislative obligations

The University of Tasmania is a State Authority of the State of Tasmania. The University has specific and implied requirements for recordkeeping. These may be further extended by related financial and administrative legislation which requires University employees to be accountable for their actions.

There are a large number of Acts which apply to the University. Those specifically relating to recordkeeping requirements include:

- University of Tasmania Act 1992
- Archives Act 1983
- Archives Regulations 2004
- Electronic Transactions Act 2000
- Evidence Act 2001
- Financial Management and Audit Act 1990
- Financial Management and Audit Regulations 2003
- Limitation Act 1974
- Personal Information Protection Act 2004
- Right to Information Act 2009
- Work Health and Safety Act 2012
- Work Health and Safety Regulations 2012.

These Acts and others govern what information must be kept, how that information must be managed and when and how the information may be disposed of. Penalties may apply for failure to comply with these requirements.
Specific information relating to the requirements of each Act may be found in Appendix I – Legislative Obligations.

3.1 Disposal Schedules, Guidelines and Advice issued by the State Archivist

The State Archivist is responsible for ensuring that State Records are managed in accordance with the Archives Act 1983. This position sits within the Tasmanian Archive and Heritage Office (TAHO).

Retention and Disposal Schedules, also known as Disposal Authorities or 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.

State Records Guidelines are a defined set of Standards for recommended practice that the University must comply with. It is the duty of the University to take all reasonable steps to ensure that the guidelines are complied with.

Information Management Advice are issued to provide advice on current recordkeeping issues and are applied by organisations as required.

Refer to the relevant sections in this document for more detail.

3.2 Identifying recordkeeping requirements

There are three main types of recordkeeping requirements:

- regulatory (or ‘accountability’ or ‘legislative’) requirements
- business (or ‘operational’) requirements
- stakeholder (government and public) expectations.

Recordkeeping requirements may be stated explicitly in laws, regulations and other instruments of authority such as Retention and Disposal Schedules and Guidelines published by TAHO, or may be implied by the environments in which the University operates.

They will refer to specific needs for evidence. For example, a requirement may state the need for:

- the creation of a record
- specific metadata associated with the record
- its retention for a specified period
- its disposal via a secure and confidential destruction method
- the records to be stored in specified conditions appropriate to its format
- access conditions/restrictions
- the record to contain specific content
- the record to be in a specific format
- aspects relating to quality that ensure it is a ‘proper’ record.
3.3 What is a record?

Records are defined by the Records Management Standard AS ISO 15489.1 (2016) as “information created, received, and maintained as evidence, and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business”.

Records can come in many different forms, including (but not limited to) paper and electronic documents, drawings, maps, plans, photographs, microforms, audio and video recordings, and database entries. It is the content that matters, not the format; if it contains evidence of business activities or transactions, it is a record.

The following are some examples of records:

- Agendas (including appendices) and minutes of meetings of formally established University boards and committees, including ad hoc committees and working parties
- Students’ academic transcripts held electronically or in hard copy format
- Decisions taken by employees under delegation which are recorded in memoranda, letters, email messages, reports etc.
- Financial transactions held electronically or in hard copy format
- Employee transactions including letters of appointment, reports on performance and other dealings between employees and the University
- Course and Unit outlines
- Applications and other forms (electronic or physical) completed by students
- Decisions conveyed to students by mail or electronically
- Lecturers’ grade lists and assignment mark lists held electronically or in hard copy
- Research grant applications
- Research ethics approvals
- Contracts / Agreements
- Master copies of University of Tasmania publications
- University Policy Framework including Policies, Procedures, and Guidelines created by the University.

3.4 When does a document become a record?

Not all documents/information are identified as a ‘record’. A document becomes a record at the point in its lifetime when it:

- is sent to others for comment, advice or approval
- contains evidence of a decision-making process
- contains evidence of business activities.

Some documents and messages such as emails are automatically records, because they are transmitted between individuals in the course of business. However, not all records will have long term value, and therefore not all need to be kept for an extended period of time.

3.5 Determining which information to capture

The importance of a piece of information is not always apparent when it is first created or received. If you answer yes to any of the questions below then the
information is to be considered as a record and captured into a recordkeeping system:

- Is there a statutory requirement to make or keep a particular record?
- Are there any financial or legal implications arising from this information that may come under investigation?
- Is this information required for reporting purposes to internal or external bodies?
- Is this evidence of a decision which sets a precedent?
- Is this evidence of a decision which will impact on another individual, office or the University as a whole?
- Is this evidence of a decision which needs or may need supporting evidence or a record of the decision and/or decision-making process?
- Is this evidence of a change to policy, procedure or methodology?
- Does the transaction have to be approved by a more senior officer, committee or specialist section?
- Does this authorise or approve an action?
- Is this formal advice or an instruction I gave or received?
- Is this information likely to be of value or importance to others outside your immediate working environment?
- Is the information likely to be of historical or cultural value to future generations?
- If I left my job tomorrow, would my successor need this information?

3.6 When to capture a record

It is always safer to capture information from its creation, rather than at a later stage. 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.

Our aim is to hold complete and accurate records and have the knowledge of their existence, who holds them, and the tools that are required to be able to retrieve these records, regardless of where in the University they are created or housed.

3.7 When to create a record

It is important to create records of conversations through telephone, video conference, SMS or face to face if significant business decisions were made and there is no documentary evidence to follow such as a letter, memo, email or other electronic message. Examples include conversations that:

- convey the primary response from the University to another organisation, an employee, a media representative or a client (i.e. instances in which a response will not be confirmed in writing), such as a verbal agreement, authorisation, directive or formal/legal advice
- represent complaints from a member of the public requiring further investigation.

Create a written record of these conversations in the form of a File Note or follow-up email and circulate it to the other participants to ensure they agree that it is an accurate reflection of the conversation.
4 Types of records

4.1 University records

All documents created, received, maintained or dispatched by University employees (including consultants and contractors) in the course of their work for the University are official University records and should be captured into a recordkeeping system. Key contextual data (metadata) should be captured immediately upon creation of a document, receipt of incoming correspondence or prior to dispatch of outgoing correspondence. This includes:

- a brief, but meaningful title
- the date the document was created/signed
- the date the document was received/despatched
- the author(s)'s name(s)
- the addressee(s)'s name(s)
- format
- security requirements (e.g. Commercial-in-Confidence)
- current location (e.g. where the records currently is/who has it)
- home location (e.g. where the record should be kept when not in use)
- required action (e.g. workflow).

4.2 Vital records

Vital records are those records that are identified as critical to returning the University back to core business functionality during or following an exceptional event such as a disaster or network failure.

Vital records protect the assets and interests of the University, its clients and stakeholders, and are usually associated with the organisation’s infrastructure, legal and financial matters. Generally these records require significant resources (e.g. time, money) to reconstruct if lost or damaged, or may be impossible to recreate altogether. Vital records typically 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 University clients and stakeholders.

Vital records may include:

- current contracts, agreements, licences, leases, titles and other signed original legal records such as grant deeds, patents, copyright, partnerships or memorandum of understanding
- research grants
- student records – enrolment and progression
- financial records and Insurance policies and schedules
- employee details including payroll and contract information
- delegations of authority
- disaster management or business continuity plans, including the vital records recovery plan
- infrastructure plans, Ordinances, Rules, operational policies and procedures.

This type of information is commonly considered to range between 5 – 10% of the total record holdings of an organisation. Vital records may be temporary or permanent, exist in any format and can be found throughout the University.
Protecting vital records should cover both measures to prevent or minimise the impact of a disaster event, and recovery and restoration measures if a disaster does occur. Where practical, the original vital record must be captured into a recordkeeping system and kept in a secure environment according to recognised standards, e.g. physical records contained in a fire proof safe. In some instances it is advisable to store the original documents off site and ensure that electronic documents are backed up regularly and stored off site.

4.2.1 Vital Records Register

Each organisational unit is responsible for identifying and maintaining a vital records register for vital records they are responsible for. This will be incorporated into a central register that will be retained by the Records Management Unit.

When registering vital records, the following details should be included for each record:

- type (e.g. brief description of record type)
- the name of the area responsible for the record service or electronic recordkeeping system containing the vital records
- explanation (e.g. brief explanation of why it is considered vital, the record’s critical purpose, consequences of loss)
- location and storage (e.g. on-site, off-site, of original, of duplicate, server, data centre, backups, mirror sites, etc.)
- date for review / update / disposal
- format (e.g. hard copy, digital, audio-visual tape, etc.)
- accessibility requirements (e.g. position, authorisation, access to storage if off-site, recovery protocols for systems, etc.).

Refer to Information Management Advice 52 – Identifying and Managing Vital Records.

4.3 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 of permanent records 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 employees and students
- contain evidence and information about activities of interest to stakeholders
- have significant potential research value.

Permanent records must be retained for 25 years, after which they are legally required to be transferred to TAHO 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.
4.4 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.

4.5 Ephemeral (short-term value) records

Ephemeral or Short-Term Value records are records which are used to facilitate University business, but are of a trivial nature or of such short-term value that they do not need to be retained once reference has ceased. It is up to each employee to systematically remove ephemeral records from email, share drives and business systems to ensure that high value records can easily be identified and retrieved. They do not need to be captured into a recordkeeping system and can be freely destroyed without listing them in a Records Destruction Request or Register of Records Destroyed. The eligible record types are listed in full in Disposal Authorisation 2158, but examples include:

- notes and calculations used solely in the preparation of other records such as correspondence, reports, budget documents, programs and tabulations
- drafts of documents relating to matters of minor importance which have not been circulated for comment/approval, do not provide evidence of significant decisions, reasons and actions or significant information not contained in the final document. Drafts which document matters such as rationale behind university policy and certain legal issues, and those drafts which are circulated for comment, should be incorporated into the recordkeeping system
- copies made from records held elsewhere in the University in any format. These include duplicate minutes, agendas, computer printouts of information contained in an electronic recordkeeping system, copies of internal circulars, abstracts or copies of formal financial records maintained for convenient reference, reference copies of film, video, microfilm or microfiche
- 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
- audio recordings that are used in preparation of other records or in preparation of minutes and transcripts of formal proceedings, not covered by any stipulation set by the University
- transmittal messages and other conversational documentation, which do not record business transactions of the university or formal communication between employees. These may include: informal transmission messages on “with compliments” slips; email and facsimile cover notes; facsimile or telephone messages of a routine or trivial nature; and informal email
- appointment diaries and meeting schedules which may be maintained on electronic systems that do not record significant matters such as notes of discussions and meetings, case notes etc.
 copies of personal documents, and 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 - such as copies of birth certificates, drivers licences, marriage certificates, copies of references, copies of qualifications, change of address notices.

Refer to RMU Information Sheet 9 – Ephemeral Records for further information.

4.6 Personal records

Personal records and correspondence are records which are of a personal nature to you and have no relevance to the business of the University. Examples include: ‘Let’s do lunch’, personal/family arrangements or CVs.

The University allows a small amount of personal information to be retained by an individual. The University has provided a specific repository, OneDrive for Business, which has superseded the P Drive to store this type of information. A folder or folders should be identified in your email inbox to identify your personal information. Business information should not be included in these personal areas.

Personal electronic documents, email and papers can be destroyed as soon as employees no longer require the information, and should be removed or destroyed prior to leaving the University.

If correspondence incorporates both personal and work-related information, then the correspondence is a University record and should be saved into a recordkeeping system.

4.7 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.

4.8 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 TAHO in accordance with University disposal procedures.

5 Record formats

5.1 Electronic records

The University conducts much of its business electronically. It is therefore necessary to create and manage information in electronic format. Electronic transactions are no different from their paper counterparts in that they need to be recorded, captured in a fixed form, maintained and made accessible as records. Electronic records must remain available, accessible, retrievable and usable for as long as a business need exists, or as long as legislative, policy and archival requirements demand, whichever is longer.

Systems and facilities should be secure from unauthorised access or modification that could result in “irrecoverable loss of records and data”. Error or equipment failure
can result in deliberate or inadvertent corruption or deletion. Back up procedures should provide a security precaution against loss, corruption and unauthorised access.

Storage media should be tested regularly to check for degradation, and information should be transferred to new storage media before loss of quality or technological obsolescence occurs.

As is the case with paper documents, not all electronic documents are records. For example, a report that has not been signed off is not a record until authorisation takes place, or it has become part of a transaction.

Any records of ongoing value which are created or received electronically, including word processed documents and emails, should be captured into a record keeping system.

Records should not be held on hard drives, USBs, CDs, DVDs or any other storage device without a strict back up regime. Once electronic documents or emails are captured into the recordkeeping system they can be deleted from your machine. The disposal of electronic documents and electronic mail must be undertaken in compliance with the Archives Act 1983.

5.1.1 Email records

Electronic records include email messages which may need to be retrieved at a later time or which have been identified as a record of the University's official work. The requirements for capture and management of email records are outlined in the Managing Email as Records brochure, State Records Guideline 7 - Managing Email as Records and State Records Advice 4 - Management and Capture of Email.

Email records, whether printed or not, are treated as documents under the Right to Information Act 2009 and are “discoverable” in litigation. They also can be produced in court by subpoena and are subject to copyright, privacy and defamation legislation. In order to maintain their value as evidence, email messages must be inviolate. This requires that they are maintained in a system which prevents them from being altered or manipulated from their original state.

Emails of ongoing value are to be captured into the corporate record keeping system (EDRMS). In offices where an EDRMS is not yet implemented, emails must either be stored in shared email folders or printed in full and placed in the physical corporate folder.

Records of business activities may only be deleted if they are authorised for destruction by the State Archivist. These authorisations will usually be issued in ‘Records Retention and Disposal Schedules’ and will apply to records irrespective of their format.

Capture key emails as soon as possible after you send or receive them, rather than waiting until the end of the email thread. Although the final email in a thread may quote the previous emails, this is by no means certain if the thread branches and there is no way of determining whether the quoted text was altered from the original.

5.1.2 Websites

The University website is not a recordkeeping system as it only retains the information for the period it is published. University websites have similar retention
rules to those for publications and as such, must be maintained and preserved. Information published on the web such as policy, procedures and guidelines must be captured into a recordkeeping system. The record must be updated each time a new version is published.

Please refer to the State Records Guideline 15 - Recordkeeping for Websites and Web Pages and the University Web Services – Policies and Standards web page for further information.

5.1.3 Web-based services and Cloud hosted services

Web based services and cloud hosted services are about using technology to create, share and exchange ideas, knowledge and information. These include but are not limited to:

- web-based services hosted on external servers with third parties such as:
  - social networking sites including Facebook, LinkedIn, Google+
  - media sharing services including YouTube, Flickr, Pinterest, Tumblr
  - blogs (e.g. Blogger, WordPress)
  - micro-blogs (e.g. Twitter)
  - wikis and online collaborations (e.g. Wikipedia)
  - forums, discussion boards and groups including Google Groups, Whirlpool
  - vodcasts and podcasts
  - instant messaging, including Facebook Chat and Skype
  - social bookmarking
  - geo-spatial tagging including Google Maps
  - online surveys including Survey Monkey
  - streaming media
- platforms supporting crowdsourcing social media hosted within the University, such as:
  - Yammer
- University systems such as:
  - intranets (e.g. internal forums, discussion boards)
  - blogs hosted by University business areas.

Social media applications are typically:

- third party owned
- located in the cloud
- subject to regular change, and
- unable to be relied upon to maintain business information to meet business and legislative requirements.

Any of these mediums may create University business records and care must be taken to ensure that any records are managed as such. Considerations include:

- Was it made, sent or received in the course of business?
- Does it record a decision taken?
- Does it record advice given?
- Does it require the process of arriving at a decision?
- Is it required to be kept by legislation?
University business areas intending to use social media must identify their high risk business processes, the systems that support these, and ensure these systems can make and keep records to document and support these high risk processes.

University business areas must conduct risk assessments both of the platform limitations and the intended content for distribution, as the adoption of these technologies may involve some risk to the integrity, security and long term preservation of records. These risk assessments should be undertaken on a case-by-case basis, and documented in a risk management plan, including strategies to export information (where appropriate) for maintenance in corporate systems.

5.1.4 Distribution and publication of electronic records

The distribution and publication of electronic records must be conducted in accordance with Ordinance 18 - Intellectual Property and associated procedures of the University of Tasmania.

Where the master set of University publications are held in electronic format, transfer the final version to the State Library of Tasmania’s Stable Tasmanian Open Repository Service (STORS).

Refer to the Publications section for further clarification.

5.2 Paper records

Paper is still a popular format for records retained in the University and even organisational units that now largely conduct their business electronically often have legacy records in paper format. Paper records need to be recorded, captured in a fixed form, maintained and made accessible as records. Paper records must remain available, accessible, retrievable and usable for as long as a business need exists, or as long as legislative, policy and archival requirements provide, whichever is longer.

These records may consist of paper documents enclosed in a manila file or folder cover and should be kept in suitable storage mediums such as lateral filing cabinets in accordance with storage standards applicable to their needs. Paper records identified as permanent in value (e.g. signed Council Minute papers) are to be printed on archival quality paper and stored in acid-free folders and boxes to ensure they remain accessible and legible over time.

5.2.1 Facsimile transmissions

Thermal fax machines utilised by the University in the 1980’s printed on thermal fax paper, which is acidic and prone to severe and rapid deterioration. Physical folders that are to be retained permanently must be checked to ensure that the thermal paper has been replaced by a photocopy of the original facsimile before transfer to secondary storage or TAHO Repository.

If the original letter was received, the fax copy should be superseded if it hasn’t been annotated. It may be noted on the original (or in the notes field in the EDRMS) that the fax was received, including date and time, and then the original fax may be destroyed appropriately.

5.3 Source records

Source records are documents or other records that have been copied, converted or migrated to a new format or system, 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, conversation or migration process.

5.3.1 Reproduction conditions for digitising source records

The University must ensure that certain conditions are met to ensure that the reproductions of records that have been digitised have the required degree of authenticity, integrity, accuracy and usability.

A documented records digitisation program must be put in place to provide evidence of due process to satisfy compliance with Disposal Authorisation No 2159. This will include establishing:

- reproduction standards
- management of the reproductions
- Quality Assurance
- storing of reproductions
- destruction of source records.

For more detailed information on requirements, please refer to Information Sheet 7 – Scanning and Destroying Paper Records and Information Sheet 10 – Scanning Specifications.

Refer to Section 10.2 Preservation/protection of records - digital formats for information relating to preservation standards for superseded formats.

5.4 Publications

5.4.1 Recordkeeping Requirements

University recordkeeping retention requirements associated with University publications are included in the Disposal Schedule for Common Administrative Functions DA 2157 section 14.12.00 issued by the State Archivist.

Publications will be managed in accordance with University Disposal requirements for transfer or destruction. Those publications of significant value that have been legally deposited with the State and National Libraries, will not be required to be transferred as a State Record to TAHO.

Research publications will also be managed in compliance with any contractual obligations associated to grant funding for storage and accessibility.

5.4.2 Legal Deposits

In accordance with State and Commonwealth legislative requirements, a copy of all University publications that are sold or otherwise distributed to the public, are subject to legal deposit with the State Library and the National Library of Australia.

- **State Library** - Refer to the State Library website, [Linc – Legal Deposit](#), for instructions on how to deposit your publications in hardcopy or electronic format
- **National Library** - Refer to the [National Library of Australia Website](#) for instructions on how to deposit your publications in hardcopy or electronic format.
5.5 Research Data and Materials

Research Data and Materials will be managed, stored and retained in accordance with the University Management of Research Data Policy and the University Management of Research Data Procedure.

Minimum retention requirements are also included in the Records Retention and Disposal Schedule for Functional records of the University of Tasmania, DA 2398 Section 19 Research Management, and will be managed in accordance with University Disposal requirements.

6 Managing records

6.1 Who owns University records?

The University owns all records created and received by individual employees as part of their day to day business. This includes research data, teaching materials and correspondence.

6.2 Who manages University records?

The majority of University records are managed by the various organisational units of the University that deal with the contents or subject matter of the records. For example, Human Resources retain and manage all employee records, while the Student Operations is responsible for examination records.

Each organisational unit is responsible for developing a records management program which provides governance around the information that they create, receive, manage and store. This program should consist of internal policies and procedures, an induction process, training and awareness raising, tools and support mechanisms for employees.

6.3 Folders

Folders are created to house documents that have common subject matter, security and retention values in the same location. They may be physical, electronic, or a combination of both, often referred to as hybrid folders. Documents are contained in a folder to ensure that they are:

- protected against loss and/or deterioration
- registered using a classification scheme (controlled language) to aid retrieval
- classified with a records disposal schedule to assist with the retention and disposal decisions
- tracked to ensure that the folder is easily retrievable
- made available for future reference.

6.3.1 Physical folders

Usually information will start its life enclosed on a generic folder until it merits a dedicated folder of its own. A physical folder should have the following features:

- the block of pages is no thicker than 2.5 cm
- all the pages are of uniform size
- all the pages are aligned
- there is nothing on the file that is bigger than the cover
• there are no folded items in the file.

Folder contents are reviewed to identify issues that have developed to the point where a new folder for the subset material is created. This reduces the amount of folders that need to be physically created and managed. It also helps when assessing the disposal or retention of the information.

If you do not have access to an Electronic Document and Records Management System (EDRMS), it is recommended that original documents are not handed loose to officers, but are enclosed on a folder and handed to the officer or forwarded electronically. This practice reduces the risk of the loss of the document.

6.3.2 Electronic folders

Electronic folders are created and managed in the same way as physical folders. University business records should be held in an EDRMS, or a compliant business information system or, if unavailable, in share folders or wikis which are identified and listed (indexed). Business information is not to be kept in personal drives or hard drives (e.g. C:/), in order to ensure that information can be shared within the organisational unit where appropriate.

Consistent naming conventions should be utilised for the naming of folders, thereby ensuring that information is retrievable. The University Business Classification scheme provides key terms and is associated to the retention requirements of the information contained in a folder.

Refer to Information Sheet 11 – Storing records in shared drives and Information Sheet 14 – Storing records in wikis.

6.4 Transfer of University records to other organisations/institutions

The custody or ownership of University records may not be changed without prior approval from the State Archivist. Where practical, it is preferable that the University retain ownership of the records, thereby retaining control of the records.

6.5 Outsourcing – Recordkeeping issues

Outsourcing of University functions may be authorised by one of two means: through the use of a legislative instrument or through a contract with a third party entity. An example of the outsourcing of University functions and activities is the outsourcing of off-site storage facilities for University inactive records.

When outsourcing University functions and activities, it is important to ensure that recordkeeping clauses are included in contracts and agreements ensuring:

• records are adequately controlled for the duration of contracts or agreements regulating the outsourcing of the University’s functions and activities
• records are disposed of legally during the outsourcing of University functions and activities
• access to records is regulated and controlled following the outsourcing of the University’s functions and activities
• the storage of records is clarified during planning and implementation of the outsourcing of the University’s functions and activities
• the ownership of records is clarified during planning and implementation of the outsourcing of the University’s functions and activities.
For specific requirements refer to the State Records Guideline 10 - Outsourcing of Government Business – Recordkeeping Issues.

6.6 Privatisation – Recordkeeping issues

The privatisation of certain functions and activities of the University may be authorised by either the use of a legislative instrument or through a contract with a third party entity.

When privatising any University functions or activities it is important to ensure that:

- State records are adequately controlled during the privatisation processes
- State records are disposed of legally during the privatisation of the University’s functions and activities
- access to State records is regulated and controlled following the privatisation of the University’s functions and activities
- the storage of State records is clarified and documented during the planning and implementation of privatisation of the University’s functions and activities
- the ownership of records is clarified during the planning and implementation of privatisation of the University’s functions and activities.

For specific requirements refer to the State Records Guideline 14 - Privatisation of Government Business – Recordkeeping Issues.

7 Recordkeeping Systems

7.1 What is a recordkeeping system?

A recordkeeping system is a system which captures, manages and provides access to records through time. These systems can be either in electronic or paper form.

A recordkeeping system should:

- routinely capture all records within the scope of the business activity it covers
- organise the records in a way that reflects the business processes of the records creator
- protect the records from unauthorised alteration, destruction or transfer
- routinely function as the primary source of information about actions that are documented in the records
- provide an audit trail of who has viewed or altered a record, and when
- provide ready access to all relevant records and related metadata.

A recordkeeping system should have accurately documented policies, assigned responsibilities and formal methodologies for its management.

Some areas of the University have access to an Electronic Document and Records Management System (EDRMS). This system assists the management of information, both physical and electronic, including email, from creation or receipt to destruction or archiving. Control processes include classification and document registration, correspondence management, folder and action tracking, security and access, retention and disposal, auditing and archiving.

Refer to Information Sheet 15 – Recordkeeping Requirements for Information Systems for further information.
7.2 What is recordkeeping metadata?

Recordkeeping metadata enables you to describe records, people and business activities in sufficient detail to ensure:

- better information accessibility
- improved records management
- greater accountability in business operations
- the context surrounding records is preserved

A number of everyday activities involve the capture of metadata about records or rely on metadata being available. Examples include:

- identifying personal information that must be protected under Privacy legislation
- accessing documents sought under Right to Information legislation
- transferring records to another organisation as a result of administrative change or privatisation
- tracking correspondence
- identifying vital records as part of disaster planning
- transferring permanent records to TAHO
- documenting the destruction of records

Metadata is a way of codifying information needed to use and access records. Descriptive metadata describes a resource for purposes such as discovery and identification. The questions below document five elements of information:

- What records do we have?
- Where are the records?
- What do the records relate to?
- Who can access the records?
- How are the records managed?

These elements are presented in tables which contain:

- a code (numeric and/or alphabetical) that uniquely identifies the element or qualifier
- the title of the element or qualifier
- the purpose of the element or qualifier
- examples and comments on how to use the element or qualifier

The State Archivist has endorsed the Recordkeeping Metadata Standard for Commonwealth Agencies and promotes this standard.

Refer to State Records Advice 14 - Recordkeeping Metadata Standard

7.3 What is a classification scheme?

Classification is the process of grouping related records together based on the business functions and activities of an organisation. It is used to name and describe specific folders that contain like subject matter, in addition to specific subject matter terms.

A classification scheme stipulates the use of controlled vocabulary to ensure that terms are used consistently. This facilitates searching, retrieval, disposal sentencing and reporting. To provide a consistent method for the classification of documents and
folders, the University has implemented the University of Tasmania Business Classification Scheme (BCS) as the basis for its classification system.

The BCS is a hierarchy of pre-defined terms, moving from broad business functions to more specific business activities. The functions represent the core operational and administrative business of the University, and each function has a subset of activities which are undertaken as part of the function. There are clear descriptions for the functions and activities. Cross-references have been added to direct users to other related terms or more appropriate terms.

The selection of the relevant terms from the classification in conjunction with a free text element provides the folder title.

Function + Activity (Sub-Activity) + Free Text Title = folder title

EXAMPLE: COURSES AND UNITS – Assessment – Coursework and Assignments – XYZ Unit.

The BCS is available through the Records Management Unit web page.

7.4 What is the disposition of a record?

A disposition describes what the current status is for a record or group of records. A disposition is another way of categorising records to enable easier retrievability of records. These are broken up into 4 categories:

- **Active** – active records are records that are used on a day to day basis, usually current. These records are kept in current folders, (electronic or physical) for easy access.
- **Inactive** – inactive records are records that have little if any business use, but are required to be retained before destruction or disposal. These records may be located in a nominated secondary storage area, be it physical or electronic.
- **Destroyed** – Destroyed records have been destroyed in accordance with the Archives Act 1983.
- ** Archived** – Archived records are records that have been identified as permanent in value and located in a controlled long term storage repository.

8 Access and security of records

All officers must be able to access the business records created by the University that they require to conduct their operational requirements of their business role. There may be specific legislation and policies that govern accessibility of some information. Records that contain personal, commercial or operationally sensitive information will be identified, labelled and restricted to ensure that only those officers that have a business reason to access this information will be able to do so.

All University records made by any employee of the University in the course of her or his duties that are not considered open to the public domain must not be divulged or released to unauthorised persons without authorisation from the employee’s Supervisor.

Release of personal information relating to employees or students is only permissible in compliance with established University policies and guidelines, as set out in the University's Privacy Policy.
Employees are required to use discretion in regard to the divulgence or release of ephemeral information. If in doubt, employees must consult their Supervisor.

Refer to the Records Security Guidelines and the EDRMS Security Guidelines for specific security requirements, clarification and risk assessment protocols.

8.1 Folders and documents

Physical records are not to be sent out or taken off campus without authorisation. It is preferable that copies be made for this purpose and identified as such. Where original records are required (e.g. for legal matters in the case of litigation) the Head of the Organisational unit and/or Manager, Records and Information should be advised before the records leave the University, to ensure appropriate record security and tracking can be completed, and follow ups for return of folders can be made.

Digital records need to be protected against unauthorised disclosure with careful consideration of where and how this information is stored or transmitted. Refer to the Records Security Guidelines for further details.

All University records must be captured into a recordkeeping system and retained with the organisational unit.

Protocols and procedures need to be implemented for employees that work from home/off-site to ensure security and access of records is managed appropriately.

8.2 University archived records held by the Tasmanian Archive and Heritage Office

University records identified as having permanent retention value have been transferred to the TAHO repository located at Berriedale. The majority of information held is over 25 years old. Listings of all records that the University has transferred are available from the Archives Online database.

When making requests to TAHO, the following information should be provided:

- Name of Organisational unit
- Requesting Officer's details (name, phone and fax numbers and email address)
- Collection details
- Item/s required (file number, file title, document title)
- Series number/s (should be provided where possible).

The series number can be found on the Archives Online database. For records that have been transferred and do not have an Accession reference, this may be obtained from the Manager, Records and Information.

Public access to restricted records that are retained by the TAHO must be referred back to the responsible organisational unit prior to release. Refer to the Public Access to Restricted Archived University Records Procedure and the associated Access to University Archival Records Confidentiality Undertaking form.

For specific requirements refer to the Advice 11 - Short Term Retrieval of State Records and Advice 23 – Government Agencies using Records in the History Room for further information.
8.3 Breaches of access and/or security

Any access or security breach must be reported immediately to a Supervisor/Manager who will refer the breach to the Director, Audit and Risk. A breach includes the loss (misplacement, unauthorised deletion or theft), inappropriate access or unauthorised disclosure of University records and information.

Any breach will be dealt with in accordance with:

- ICT Services and Facilities Use Agreement and Policy
- University of Tasmania Staff Agreement

9 Storage of Records

Records are required to be stored on appropriate media or hardware, and in appropriate formats, and are required to be stored in suitable containers, locations and systems.

The University is required to implement storage management strategies including:

- Disaster Management plans
- Vital Records plans
- Digital records management.

The University is required to monitor records storage for environmental conditions appropriate to the media, and retention periods.

The University is required to store and handle records according to their security status.

Where storage is outsourced, only approved secondary storage providers must be used by the University.

9.1 Storage of Confidential and Sensitive records

Every organisational unit is required to develop and implement protocols and procedures to appropriately store, manage and protect sensitive or confidential records, regardless of format, from unauthorised access, damage and loss (including theft).

Some of the more sensitive records include:

- student records
- client records
- medical records
- employee records
- Right to Information requests
- grievance matters
- legal matters
- performance appraisals
- tender documents.

If you require access to records you would not normally have access to, you must formally request access from the relevant owner of the records through your supervisor.
Refer to the Records Security Guidelines for specific storage requirements.

9.2 Physical storage

Organisational units are responsible for the management and monitoring of storage repositories for active and inactive physical records. All inactive records should be listed in a Register of Inactive Records prior to transfer to an approved secondary storage provider.

Where possible, all physical records storage areas are to be secure areas with access only provided to authorised personnel. Employees are not permitted to access records for which they have no authorisation. Where a secure storage area is unavailable, all University physical records should be stored in lockable shelving units to prevent unauthorised access when offices are unattended during the day or after hours. Employees must ensure shelving units are locked appropriately, and confidential and/or sensitive records are not left on desktops or in plain view whilst offices are unattended.

Records must be stored in conditions that ensure they are accessible and retrievable in appropriate timeliness for the length of time they are retained. Records should be stored in conditions that take into account their physical characteristics, sensitivity, retention period and expected access rate.

Storage facilities used must comply with work health and safety guidelines as adopted by the University. Storage facilities that are provided by commercial storage providers are required to be certified as an approved secondary storage provider by TAHO.

Disaster management plans should include protocols and procedures for responding to disasters identified as risks to those storage areas.

Refer to State Records Guideline 11 – Physical storage of State Records and RMU Information Sheet 1: Managing Inactive Records.

9.3 Electronic storage

Media or hardware storage should be appropriate to the record format, retention period, security protection and storage capacity requirements. Equipment or technology dependant records are to remain accessible for as long as they are required (e.g. audio-visual material and magnetic tapes). Preservation strategies may involve refreshing, converting or migrating stored records into different formats. Permanent records must be stored in the best possible conditions while in the custody of the University to ensure their long term preservation and access.

Digital records storage should be regularly monitored for any media decay and to regularly assess ongoing viability of file formats and storage media or hardware.

Business systems where records are stored are required to have recordkeeping functionality to ensure that the records are authentic, accurate, secure and accessible for as long as they are required to be retained.

The University uses many business information systems which stores records, such as TechOne, Student Management, the Research Management Database and Archibus. Some of these systems do possess the requisite functionality to be used as a recordkeeping system, but all University systems are to be assessed against recordkeeping requirements.
Confidential and sensitive information must be identified and protected from unauthorised access, alteration or deletion by ensuring that appropriate security measures are put in place to deal with this type of information. Measures may include:

- setting up work group access to directories/folders
- locking the machine if absent from the office
- utilisation of passwords
- making documents ‘read only’
- ensuring ‘records’ are identified as such and placed into an EDRMS, or a compliant business system.

### 9.4 Using shared folders in conjunction with a recordkeeping system

Shared folders are utilised to facilitate collaboration and dissemination of information, and to store certain document formats that are difficult to capture into a recordkeeping system. These shared folders can be either located on network drives or in shared email accounts set up for a workgroup or organisational unit.

Shared folders are a useful tool, but they are not a recordkeeping system and should be used in conjunction with a recordkeeping system such as an EDRMS where possible. If shared folders are used to store electronic records, they need to be managed and monitored regularly to ensure that proper records are kept. Some of the ways in which this can be achieved include the following:

- Incorporate the use of shared folders into the overall information management framework, e.g. setting up a controlled folder structure based on the University of Tasmania Business Classification Scheme
- Provide viable alternatives for employees to use instead of shared folders. These include an easy to use recordkeeping system and collaboration tools, and the use of an intranet to facilitate dissemination of documents
- Ensure that copies of all approved or final versions of documents are placed into a recordkeeping system
- Ensure that all employees are aware that the “official” version of the documents should be obtained from the recordkeeping system
- Provide links between the shared folder and the recordkeeping system
- Change work practices to ensure that draft documents are removed from the shared folder after being placed into the recordkeeping system
- Remove out of date or obsolete drafts or reference copies of documents from the shared folders on a regular basis. This can be assisted by including version control in headers and file paths in footer in documents
- Enforce security permissions that limit the ability of most users to create folders and delete or amend documents
- Ensure that your recordkeeping policy and procedures cover the use of shared folders.

From a recordkeeping perspective, shared folders have some of the following risks:

- It is easy to develop a confused, uncontrolled hierarchy of folders and document titles, making retrieval difficult
- The lack of recordkeeping functionality means that documents are not ‘good’ records nor reliable evidence
It is difficult to collect recordkeeping metadata that identifies, authenticates and describes records in a systematic and consistent way.

Security settings that permit users to save documents to the folder also give users the ability to inadvertently delete a document.

Ease of alteration (either deliberate or accidental) makes it difficult to ensure that the version in the shared folders is the same as the ‘official’ version. Audit trails detailing alterations are not usually kept.

Ease of duplication means that it is difficult to identify where the ‘primary’ record is located.

The overall management of documents is generally ‘ad hoc’ and not incorporated into the overall information strategy of an organisation.

It is difficult to identify sequences of documents (either within the shared folder, or in other systems) that relate to the one business process.

Limited capacity of information technology infrastructure may mean there is pressure to destroy documents while they are still useful.

For further information refer to Information Sheet 11 – Storing records in shared drives and State Recordkeeping Advice 41 – Managing Records on Shared Network Drives and Advice 42 - Structuring Shared Network Drives for Recordkeeping.

9.5 Off-site storage of inactive records

Commercial off-site storage facilities may be utilised for storage of inactive records waiting destruction or transfer to TAHO. Consideration of the specific requirements for the type of records needs to be factored into choosing a suitable storage service provider. Paper has different environmental storage requirements compared to magnetic tape or photographic film, specimens or ice core samples.

The commercial service provider you choose must be a certified Approved Secondary Storage Provider (ASSP) and the certification approved by the State Archivist. Certification will be renewed every 12 months.

When entering into arrangements to store University inactive records with a service provider, both parties must articulate their roles and expectations in the service contract. All contractual arrangements must recognise their continuing responsibility for the proper management of those records including consideration of liability and insurance issues.

Refer to State Records Guideline 13 – Certification for secondary storage providers for the certification requirements and checklist and a list of ISO Storage Standards.

Irrespective of where they are stored, State records are subject to legislation such as the Right to Information Act 2009 and to legal processes such as discovery and subpoenas.

A Register of Inactive Records listing all records must be retained by the transferring organisational unit to ensure that the records are easy to retrieve. Ideally these records should be appraised and scheduled before transfer so disposal or transfer can be undertaken in an efficient, cost effective timely manner.

Refer to RMU Information Sheet 1 – Managing Inactive Records and Information Sheet 12 – Off-Site Document Storage Providers.

Refer to State Records Guideline 13 – Certification for secondary storage providers and State Records Guideline 11 - Physical Storage of State Records.
9.6 Storing records in the Cloud

Cloud computing involves the transfer to or creation of content in data stores which are maintained by a service provider, and are geographically remote from the customer. Where University business is undertaken using cloud computing these data stores will contain University records.

A risk assessment is required to be undertaken prior to the University entering into any arrangement with a cloud computing service provider. Consideration should be undertaken in relation to the implications of:

- sending or storing information outside the state or country
- unauthorised access
- loss of access
- unlawful disposal
- security and access of records
- community expectations.

The process of selecting a cloud service provider should be rigorous to ensure the provider meets your specific recordkeeping requirements based on your risk assessment. This should then be followed up by entering into a contractual arrangement prior to records being transferred to the cloud storage provider.

Ongoing monitoring of the cloud service provider is required to ensure that your information management objectives are being met, including the identification of any arising risks that may not have been realised at the time of entering into the initial contract.

The University has formal agreements for the following cloud based storage repositories that also can be utilised for sharing large files:

- OneDrive for Business – OneDrive for Business is an integral part of Office 365 or SharePoint Server, and provides place in the cloud where you can store, share, and sync your work files. You can update and share your files from any device with OneDrive for Business. You can even work on Office documents with others at the same time.

- CloudStore - is a web service provided for the secure transfer of large files. No software or additional configuration is required for University of Tasmania members. To access this service, logon using your University username and password.

- eResearch Ecosystem - delivers both a high performance computer and a secure research data storage platform to local, national and international research collaborators.

DropBox is not a preferred option for storage and/or transfer of University business information.

Refer to State Records Guideline 17 – Managing the recordkeeping risks associated with cloud computing.

10 Preservation/protection of records

Records appraised as requiring permanent or long term retention need to be retained in a more stable environment and format than records requiring only short-medium term retention.
Storage conditions and handling processes should ensure as far as possible that records are protected from unauthorised access, loss, destruction, and from theft and disaster.

10.1 Physical Records

Major causes of deterioration of physical records in their various formats are light, heat and humidity, handling, mould and pest infestation. Most of these factors can be avoided by controlling the environment in which physical records are stored:

- Storage areas are to be kept free of dust by regular cleaning
- Conduct regular inspections for pest infestation and fumigate as required
- Paper records should ideally be stored in areas that do not have great fluctuations of temperature or humidity. An acceptable temperature range for paper is 18-20 °C with a relative humidity between 45-50%. The recommended temperature for Magnetic media such as tape, floppy or hard disks is the same as for paper, but the recommended relative humidity is 35-45%. Photographs require a temperature range between 18-22 °C with a relative humidity of 45-55%.
- Records should not be placed in direct sunlight
- Metal clips/fasteners are not recommended, as they have a tendency to rust over time
- Care should be taken at all times when dealing with records
- Storage areas should be selected that have plenty of ventilation and no damp
- Damage to the immediate area, such as cracks in walls, floors or ceilings, should be repaired promptly
- The paper quality of records of a permanent value should be considered. Cheaper papers tend to contain a higher acid content, which reduces the life expectancy of the paper. Recycled paper has a life expectancy of approximately 10 years. Archival quality acid-free paper is available and is recommended for records requiring permanent retention
- Archival quality boxes are produced from an archival corrugated board. This blue-grey coloured board is acid free and made to high standards of strength and permanence set by the TAHO. These boxes are available in many sizes, but be aware that Type 1 (17x25x38cm) is the preferred option by TAHO. For temporary paper records, craft board archive boxes may be used, but "reflex" boxes are not suitable
- Master Sets of Maps and Drawings should ideally be stored in purpose built Hanging Cabinets
- A4 Ring Binders are not suitable for long term retention; records can be easily transferred from ring binders by using the Liftboy system or mediclips.

10.2 Digital formats

TAHO recommend that high value, permanent and long term records are either created in a recommended format, or migrated shortly after their creation or shortly after their active business use has ceased.

The approach to digital preservation must ensure:

- the content of the record remains unchanged despite preservation processes
- an appropriate audit trail of preservation activities is recorded
- compliance with digital recordkeeping standards of authenticity.

Storing audio-visual records such as microfilm, microfiche, photographs, magnetic tapes and floppy and hard disks requires more specialist treatment than that required for paper records. To ensure that digital records are accessible over time, migratory plans and processes need to be put into place. Refer to TAHO State Records Guideline 8 - Management of Source Records that have been Copied, Converted or Migrated.

Research specimens and collections will require specialist storage suited to the type of material being stored.

Refer to TAHO State Records Guideline 11 - Physical Storage of State Records for clarification on standards.

Refer to TAHO State Recordkeeping Advice 48 –Treating Records with Mould for advice regarding checking for and treating mould infestations.

See Appendix 2 for recommended storage media for physical/paper records.

If records of value need conservation, advice can be sought from TAHO Conservation Section.

11 Disposal of records

Disposal, which includes both the destruction and transfer of records, applies to records in all formats. The prompt, secure and lawful disposal of non-current records is essential to support accountable and efficient records management.

Records disposal must be approved by the State Archivist.

The University must develop and maintain an approved Retention and Disposal Schedule, covering all unique university-specific functions.

Records destruction must be secure, documented and appropriate to the media.

The University must have an active disposal program.

Custody of records must be appropriately managed during administrative change.

Disposal of source records must meet TAHO requirements.

The University must not decommission or migrate business systems without consulting the TAHO.

Permanent records must be retained in the University for no longer than 25 years and then transferred to the TAHO (unless an exemption has been granted by the State Archivist).

11.1 Records Disposal Program

Each Organisational Unit is responsible for implementing a records disposal program for ensuring records are routinely disposed of in accordance with University disposal requirements. This includes documenting and promulgating internal processes and procedures specific to your organisational unit. Disposal programs will include:
11.2 Appraisal of records

Appraisal is the process of evaluating the University’s business activities to determine which records need to be created and captured into recordkeeping systems, and how long the records need to be kept to meet business needs, the requirements of organisational accountability, and community expectations. This includes determining which records should be kept as part of our University’s collective memory and cultural heritage.

Decisions on how long records should be retained are based on the recordkeeping requirements of the record. In addition to regulatory, business and stakeholder requirements, the potential research value of the records should also be considered, as this is a significant aspect of community stakeholder expectations. Many records created for a specific purpose have a research value unrelated to the reason for their creation.

Records identified for permanent retention are likely to be those which:

- provide evidence and information about the University’s policies and actions
- provide evidence and information about the University’s interaction with the client community it serves
- document the rights and obligations of individuals and business areas
- contribute to the building of the University’s memory for scientific, cultural and historical purposes
- contain evidence and information about activities of interest to internal and external stakeholders.

To ensure accountability, it is essential that the processes identifying recordkeeping requirements are well documented and provide the necessary detail to justify the disposal recommendations submitted to the State Archivist. This is accomplished by drafting or amending functional disposal schedules or when making one-off recommendations for the disposal of unscheduled records. The documentation should provide the rationale for each requirement and enable it to be traced back to its source.

Refer to the TAHO Information Management Advice 2 – Records Appraisal for further detail.

11.3 Disposal authorisation

Authority to dispose of records must be obtained from the State Archivist before destruction or transfer. This can be undertaken by either:

- implementing disposal actions identified in approved Disposal Schedules, or
- obtaining written authorisation from the State Archivist for those items not covered by a Disposal Schedule.
11.4 Retention and Disposal Schedules

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.

The following schedules are applicable to the University:

- **Disposal Schedule for Common Administrative Functions Disposal Authorisation No. 2157** ([DA 2157](#))
- **Disposal Schedule for Short-Term Value Records Disposal Authorisation No. 2158** ([DA 2158](#))
- **Disposal Schedule for Temporary Value Source Records Disposal Authorisation No 2159** ([DA 2159](#))
- **Retention and Disposal Schedule for Functional Records of the University** ([DA 2398](#))
- **Disposal Schedule for Training and Assessment Records of Government Registered Training Authorities No 2135** ([DA 2135](#)).

Refer to [Information Sheet 4 – Disposal Schedules](#).

11.5 Unscheduled records

Unscheduled records are University records that are not described in any of the disposal classes listed in current 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. When seeking to destroy unscheduled records rather than transfer them, the Application must be accompanied by a completed Destruction Authority checklist. This procedure should only be used in circumstances when the records need to be disposed of as a priority and it is impractical to develop or amend a disposal schedule.

Refer to [Information Sheet 5 – Unscheduled Records](#) and the [State Recordkeeping Advice 10 - Disposal of Unscheduled Records](#).

11.6 Destruction

With the exception of ephemeral (short term value) records, records need to be registered in a Records Destruction Request form prior to destruction. Once approved, records can be physically destroyed in accordance with their format requirements.

Items listed in the Records Destruction request form that have been destroyed are to be transferred into the Register of Records Destroyed, which is signed off annually by the Head of the Organisational Unit and submitted to the Records Management Unit for audit purposes.

Refer to [State Records Guideline 21 – Approved destruction methods for State Records](#).
11.6.1 Records Destruction Requests

All scheduled records due for destruction, with the exception of those scheduled under the Disposal Schedule for Short-Term Value Records (DA 2158), are to be listed in a Records Destruction Request form and emailed to the Records Management Unit. The request must be approved by the RMU before the records may be destroyed. There is no need to list ephemeral records in a Records Destruction Request before destroying them. For records not covered by a Disposal Schedule, you should seek authorisation from the State Archivist before destruction can proceed. Refer to the section on Unscheduled Records for further details.

Records relating to imminent or ongoing legal action, government investigations or inquiries, or Native Title claims are also subject to restrictions and may not be destroyed until the matter has been resolved. Records relating to indigenous families and communities or which document links between indigenous people and localities are not to be destroyed, and should be the subject of consultation with TAHO.

Refer to Information Sheet 3 – Destroying Records and the Records Destruction Request form.

11.6.2 Registers of Records Destroyed

Each University organisational unit is required to create and maintain Registers of Records Destroyed documenting the destruction of their records. Registers of Records Destroyed are central to the accountability process built into the disposal schedules and must be signed by the head of the relevant organisational unit.

It is important to recognise that the formal evidential record of destruction is contained in this registration process. As these registers must be made available to the State Archivist (or nominee) on request, organisational units are required to forward copies of their completed registers to the Records Management Unit after they are signed.

It is expected that destruction authorised by the Disposal Schedule for Short-term Value Records – DA 2158 will be a normal administrative practice and therefore it is not necessary to make an entry for these records in a Register of Records Destroyed.

Registers of Records Destroyed should not be used to list unscheduled records, as these will be covered by a Destruction Authority issued by the State Archivist.

Refer to the University’s Register of Records Destroyed form from the Records Management Unit’s web site and the associated Information Sheet 3 – Destroying Records.

Records that have been approved for destruction under a relevant disposal schedule or authority should be destroyed in accordance with the following recommendations for the medium in which the record exists. The University must ensure that these records and any copies are destroyed and that the process is confidential and secure. The responsibility for authorising destruction is delegated to the Heads of the organisational units which own the records.

11.6.3 Destroying paper records

Depending on the degree of confidentiality and the volume of material, three methods are available for the disposal of paper records after destruction has been authorised:
• The records may be placed in large containers supplied by a University endorsed commercial waste management firm for security shredding. These large containers should be located in a secure location, or alternatively have locks so documents cannot be removed.
• Individual sheets may be passed through a paper shredder.
• Ephemeral material may be recycled by pulping or normal waste disposal processes depending on amount/bulk.

11.6.4 Destroying electronic records

When deleting electronic records, employees will need to ensure that information is wiped clean or physically destroyed. Deleting records in some programs does not actually remove the information. Most operating systems do not erase deleted information from hard disks, but simply remove the file names from the directory and eventually write over the unwanted information.

Hard disks of computers and other magnetic media should be reformatted to ensure the data is removed before computers are disposed of.

Refer to the Secure Disposal of ICT Equipment Procedure.

Refer to State Records Guideline 21 – Approved destruction methods for State Records

11.7 Transfer

11.7.1 Permanent records

Permanent records should be transferred to TAHO 25 years after the last action or transaction is completed. The Archives Act 1983 establishes 25 years as the maximum required timeframe for the transfer of permanent records to TAHO unless an extension of time has been approved by the State Archivist. Currently TAHO will not accept records less than 25 years old due to storage issues.

Please liaise with TAHO in relation to electronic records that are over 25 years.

Refer to Information Sheet 6 – Permanent Records

11.7.2 Temporary records

Temporary records can be destroyed following the expiry of retention periods specified in Disposal Schedules, or by obtaining a destruction authority from the State Archivist. Temporary records can be retained by the University after their retention period has expired if required for administrative purposes, but the provisions of the Archives Act 1983 regarding their proper care and custody continue to apply while they are still in existence. Off-site storage facilities can be utilised for inactive temporary records if storage is an issue.

Refer to the Off-Site Storage of Records section in these guidelines for further details.

11.7.3 Records copied into other media

The Electronic Transactions Act 2000 facilitates electronic communications and the Evidence Act 2001 changes the requirements for admissibility of evidence for records created or maintained in electronic systems. The provisions of these two Acts do not
override the provisions in the *Archives Act 1983* that the disposal of all State Records must be authorised by the State Archivist.

Technology enables records created in one medium to be copied or converted to another medium requiring less storage space and allowing better access (e.g. paper copied to microfilm or converted to electronic format). The reproductions of source records may be retained as the official agency records providing they have the required degree of authenticity, integrity, reliability and usability necessary to substitute for the source records in business and regulatory applications. This includes their use as evidence in the Courts, to respond to Right to Information requests, or to comply with guidelines issued by the State Archivist.

The [Disposal Schedule for Source Records - DA 2159](#) covers the disposal of source records. Please refer to the [State Records Guideline 8 – Management of Source Records that have been Copied, Converted or Migrated](#) for further clarification.

### 12 Tasmanian Archive and Heritage Office (TAHO)

TAHO underwent a restructure in December 2017 and is made up of the following business units:

- The Office of the State Archivist (formally the Government Information Strategy Unit) supports state and local government in meeting their accountability requirements under the *Archives Act 1983* and work with them to identify and manage the records that form part of the State Archive. In addition they provide a framework of policy and advice to guide the creation, retention, management and access of state and local government records in Tasmania. They also develop and issue Records Disposal Schedules to ensure that records of continuing value to the public and the government are kept and are accessible for appropriate lengths of time.

- Government Archives and Preservation Unit whose role includes managing our State archives collection and working with government agencies to coordinate the transfer of permanent value records into our custody.

From a public perspective TAHO remains as the identity of its entire collection of government archives and private collections as well as the physical and online space for public access to our collections and services.

Services are located on the 2nd floor, 91 Murray St, Hobart with its main storage repository at Berriedale.

Prior to 2012, TAHO was known as the Archives Office of Tasmania.

The Vice-Chancellor is the delegated authority and is ultimately responsible to the State Archivist for the management of all University Records. The Manager, Records and Information is the nominated first point of contact for TAHO. Any communication with TAHO should include a carbon copy (cc) to the Manager, Records and Information.

### 12.1 Transfer of records to TAHO

The *Archives Act 1983* stipulates that ‘relevant authorities’, such as the University, must transfer state records more than 25 years old to TAHO unless the records have been authorised for destruction or a written exemption has been obtained from the
State Archivist. Conditions may be imposed in respect to the management of, and provision of access to, state records that are the subject of an exemption.

All records identified as having a ‘permanent’ status in an authorised Disposal Schedule should be transferred to the TAHO 25 years after the last action.

Where permanent value records are maintained in an electronic format, the issues of system changes and media and file format obsolescence and the continuing linkage of recordkeeping metadata with individual records need to be managed by the University to ensure these records remain accessible over time.

Strategies should be developed and implemented for refreshing and migrating media formats, migrating file formats, and managing recordkeeping metadata.

Refer to the State Recordkeeping Advice 12 – Preparing Records for Transfer to the Archives Office.

12.2 Access requirements for state records

Records that are transferred as State Records to TAHO will become publicly accessible when transferred unless access restrictions are notified at the time of transfer. When transferring scheduled records to TAHO, the University will need to indicate in their ‘Application to dispose of State records’ form if restrictions are required.

This recommendation will be recorded on the completed ‘Transfer and Access Agreement’, which will be returned to the University for approval once the records have been processed by the TAHO. The ‘Transfer and Access Agreement’ is signed by the University’s delegated authority, the Vice-Chancellor, and the State Archivist. It is the official form of receipt acknowledging transfer of the records listed to the custody of the State Archivist.

University records that have been transferred to TAHO and are open to public access can be requested and accessed through the Reading Room, L2 91 Murray Street, Hobart. Refer to the section on How to Access University Archived Records held by TAHO.

Public access to restricted records that are retained by TAHO must be referred back to the responsible organisational unit prior to release. Refer to Public Access to Restricted Archived University Records Procedure and the associated Access to University Archival Records Confidentiality Undertaking form.

For specific requirements refer to the following Guidelines and Advices issued by TAHO:

- State Records Guideline 4 - Agency Determination of Access Restrictions
- State Records Guideline 12 - Short-term retrieval of State Archives
- State Recordkeeping Advice 11 - Short term retrieval of State Archives.

13 Right to Information

As a public authority, the University of Tasmania is bound by the provisions of the Right to Information Act 2009 and is committed to furthering the objectives stated within it. This Act replaces the Freedom of Information Act 1991.
Any documents created and received by a University officer in the course of their duties may be subject to a Right to Information (RTI) application. University records of any format may be required to be produced in response to an RTI application including emails and electronic data stored within databases, servers, hard discs, USB’s etc.

13.1 Disposal of records with regard to the Right to Information Act 2009

The University will not be contravening the terms of the Right to Information Act 2009 by destroying records according to an approved Retention and Disposal Schedule or Authority unless a destruction hold has been put in place for specified information. A destruction hold is placed on records that have been identified as having an ongoing requirement to be retained (e.g. an ongoing investigation into a student or employee or legal proceedings).

13.2 Retention of records for Right to Information purposes

If an application made under the Right to Information Act 2009 has been received and is still being considered or is subject to internal or external review processes for which the time limits have not expired, the relevant records must be retained until the application has been finalised. If records are retained beyond their retention period, and are still in existence when an RTI application is received, the University will be required to produce those documents.

13.3 Access to archived records for Right to Information purposes

Records archived under the terms of the Archive Act 1983 will be accessible for Right to Information purposes, subject to the terms of access contained within the Right to Information Act 2009, Section 11 - Information held by Archives Office. Records placed in the custody of TAHO are still considered to be in the possession of the University for the purposes of the Right to Information Act unless they can be inspected by the public at TAHO without recourse to the Act (i.e. no access restrictions were placed on the records when they were transferred or those restrictions have now expired).

14 Privacy

All employees involved with the collection, storage and use of personal information should be familiar with the University Privacy Policy and the Personal Information Protection Act 2004. Records will be managed in compliance with security and access guidelines.

15 Responsibilities

All University employees have a responsibility to ensure University records that they create and receive as part of their business role are complete, accurate and managed in accordance with this Policy and associated Guidelines and Procedures.

The Vice Chancellor and Senior Management Team have overall responsibility for ensuring that the University fulfils its legal and business obligations in relation to recordkeeping and that adequate resources are available for managing and maintaining University records.

Heads of Organisational Units are required to facilitate and promote the establishment and resourcing of appropriate record keeping systems in accordance
with University Policy and Procedures. Heads of Organisational Units are to ensure that employees have a clear understanding of recordkeeping requirements for their business area and provide adequate training and education. They are responsible for ensuring records are disposed of in accordance with authorised disposal schedules, and for certification of entries made in each of the business units Register of Records Destroyed.

The *Records Management Unit (RMU)* is responsible for issuing policy, procedures and guidelines, education, training and advice to assist areas to conform to the requirements for University recordkeeping. The RMU is also responsible for the configuration, development, implementation, training and support for the Electronic Document and Records Management System (EDRMS) that is utilised by business areas where the system has been implemented.

*Information Technology Services* is responsible for maintaining the databases and systems on which records and information is stored including undertaking system backups and developing, maintaining and testing the University’s disaster recovery plan.
### Glossary

Please refer to the [Tasmanian Archive & Heritage Office glossary](#) for a full listing of terms.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Trail</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>Appraisal</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 functionality 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. |
| **Deletion** | 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. |
| **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. |
| **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. |
| **EDRMS** | An Electronic Document and Records Management System manages electronic and hard copy records, enabling saving, editing, locating, tracking, archiving and disposal of information in the one system. |
| **Electronic Record** | 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. |
| **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. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>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).</td>
</tr>
<tr>
<td>Inactive Record</td>
<td>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.</td>
</tr>
<tr>
<td>Indexing</td>
<td>The process of establishing access points to facilitate retrieval of records and/or information.</td>
</tr>
<tr>
<td>Information</td>
<td>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).</td>
</tr>
<tr>
<td>Inviolate Records</td>
<td>Records that are time-bound and complete. To be inviolate, a record must be securely maintained to prevent alteration and unauthorised removal.</td>
</tr>
<tr>
<td>Metadata</td>
<td>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.</td>
</tr>
<tr>
<td>See also Data</td>
<td></td>
</tr>
<tr>
<td>Migration</td>
<td>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.</td>
</tr>
<tr>
<td>Off-site storage</td>
<td>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.</td>
</tr>
<tr>
<td>Organisational Unit (OU)</td>
<td>College, Faculty, School, Discipline, Centre, University Institute, other University Entity, Division, Section or University Business Enterprise. See Business Unit.</td>
</tr>
<tr>
<td>Permanent Records</td>
<td>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.</td>
</tr>
<tr>
<td>Preservation</td>
<td>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.</td>
</tr>
<tr>
<td>Record</td>
<td>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</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Record Type</td>
<td>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.</td>
</tr>
<tr>
<td>Recordkeeping</td>
<td>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).</td>
</tr>
</tbody>
</table>
| 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 manuals, 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. |
<p>| 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. |
| Records Management Program | A records management program encompasses the management framework, the people and the systems required within an organisation to manage full and accurate records over time. This includes the identification and protection of records with enduring value that may be required as State archives. |</p>
<table>
<thead>
<tr>
<th>Registration</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>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. A central place where data is stored and maintained. A repository can be a place where multiple databases or files are located for distribution over a network, or a repository can be a location that is directly accessible to the user without having to travel across a network.</td>
</tr>
<tr>
<td>Retention and Disposal Schedule</td>
<td>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.</td>
</tr>
<tr>
<td>Retention Period</td>
<td>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</td>
</tr>
<tr>
<td>Sentencing</td>
<td>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.</td>
</tr>
<tr>
<td>Source Record</td>
<td>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.</td>
</tr>
<tr>
<td>Structured Data</td>
<td>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.</td>
</tr>
<tr>
<td>Temporary record</td>
<td>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.</td>
</tr>
<tr>
<td>TAHO</td>
<td>Tasmanian Archive and Heritage Office (incorporating the Office of the State Archivist and Government Archives and Preservation).</td>
</tr>
</tbody>
</table>
| **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. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TRIM</strong></td>
<td>Refer to EDRMS.</td>
</tr>
<tr>
<td><strong>University Employee</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>University Records</strong></td>
<td>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 Record</td>
</tr>
<tr>
<td><strong>Unscheduled Records</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Vital records</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

### Versioning

<table>
<thead>
<tr>
<th>Former Versions</th>
<th>Current Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1</td>
<td>Version 4</td>
<td>Version 5</td>
</tr>
<tr>
<td>Version 2</td>
<td>Records Management Guidelines; Reviewed September 2013; Approved (January 2018)</td>
<td></td>
</tr>
<tr>
<td>Version 3</td>
<td>Records Management Guidelines; Reviewed 2006; Approved 2010</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Records Management Guidelines; Reviewed 2017; Approved (January 2018)</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 1 – Legislative obligations

18.1 University of Tasmania Act 1992

Under the *University of Tasmania Act 1992* the University of Tasmania is responsible for various functions including:

- to advance, transmit and preserve knowledge and learning, to encourage and undertake research;
- to promote and sustain teaching and research to international standards of excellence;
- to encourage and provide opportunities for students and employees to develop and apply their knowledge and skills;
- to provide educational and research facilities appropriate to its other functions;
- to promote access to higher education having regard to principles of merit and equity;
- to foster or promote the commercialisation of any intellectual property; and
- to engage in activities which promote the social, cultural and economic welfare of the community, and to make available for those purposes the resources of the University.

These functions require the management of records for business, regulatory or stakeholder requirements as specified or implied by State or Commonwealth legislation.

18.2 Archives Act 1983 & Archives Regulations 2004

The *Archives Act 1983* and amendments, and the Archives Regulations 2004, provide the legislative background and provisions for dealings with State records and establish the framework for formal guidelines and other standards and policy settings for management of these records.

The Archives Act includes:

18.2.1 Section 10 - Preservation of State Records

1. The relevant authority, i.e. University of Tasmania –
2. is to keep proper records in respect of the business of the Government department, State authority or local authority for which the relevant authority is responsible
3. is to cause all such records to be preserved and accessible until they are dealt with in accordance with this Act
4. may, in the name of the Government department, State authority or local authority, take legal proceedings for the recovery of any such records if the relevant authority no longer has legal custody of them.
5. Where the State Archivist believes on reasonable grounds that any State records are being kept under control of a relevant authority, the State Archivist may –
6. after giving not less than two days’ notice to the authority, enter and inspect any place under the control of that authority or any place at which the State Archivist believes on reasonable grounds that any such records are being kept
7. inspect any State records kept at any place entered pursuant to paragraph (a)
8. give advice in writing to the relevant authority with respect to the keeping of any State records under the control of the authority.
9. Any person who, without lawful justification or reasonable excuse, obstructs the State Archivist in the exercise of the powers conferred by subsection (2) (a) or (b) is guilty of an offence and is liable on summary conviction to a fine not exceeding 5 penalty units.

10. It is the duty of every relevant authority to whom or to which advice is given under subsection (2) (c) to take all reasonable steps to implement the advice.

11. In subsections (2) and (3) a reference to the State Archivist includes a reference to any State Service officer or State Service employee who is for the time being acting with the authority of the State Archivist.

18.2.2 Section 10A - State Archivist may issue guidelines

12. The State Archivist may, by written instrument, issue guidelines to a relevant authority in respect of any matter relating to the making and the keeping of State records.

13. The State Archivist may, by written instrument, amend or revoke the guidelines.

14. It is the duty of the relevant authority to take all reasonable steps to ensure that the guidelines are complied with.

18.2.3 Section 20 - Disposal, destruction, &c., of State records

(1) Except as provided by this Part, a person shall not–

(a) destroy or otherwise dispose of a State record or

(b) transfer, or be a party to arrangements for the transfer of, the custody of a State record or

(c) transfer, or be a party to arrangements for the transfer of, the ownership of a State record or

(ca) refuse to provide the State Archivist with the full name and residential address of the person for whom that person is acting as an agent in an arrangement under paragraph (b) or (c) for the transfer of a State record or

(d) damage or alter a State record.

Penalty:

Fine not exceeding 50 penalty units.

18.3 Electronic Transactions Act 2000

The Electronic Transactions Act 2000 is an Act to facilitate electronic transactions. It also supports the Evidence Act 2001 by providing guidance on provision of admissibility of information and records as evidence in electronic format.

If a Commonwealth/State law requires information to be recorded in writing, an electronic record will satisfy the requirement, if at the time of recording the information, it was reasonable to expect the information would be readily accessible for subsequent reference. If the use of a particular kind of data storage device is required, that must be used.

If a Commonwealth/State law requires a written document to be kept for a particular period, an electronic version of that document will satisfy the requirement if the above
conditions are met and the method for recording it assures the integrity of the information contained in the document.

If a Commonwealth/State law requires an electronic communication to be kept for a particular period, a person retaining that information in electronic form will satisfy the requirement if all of the above conditions are met. Records must also be kept identifying the origin, destination, time of sending and time of receipt of the electronic communication.

18.4 Evidence Act 2001

Commonwealth and State Evidence Acts may impact on how records are managed in the University, as they may be subject to subpoena or court discovery. For records to be admissible they must be:

- authentic (i.e. not having been altered or modified without authority)
- complete and accurate
- logically sequenced and arranged.

18.5 Financial Management and Audit Act 1990

The Financial Management and Audit Act 1990 is an act to provide for the management of the public finances of Tasmania in an economical, efficient and effective manner consistent with contemporary accounting standards and financial practices, for the audit of public finances.

18.6 Financial Management and Audit Regulations 2003

These regulations replace the Financial Management and Audit Regulations 1990; they –

(a) provide for the payment and calculation of State Service salaries and allowances; and

(b) prescribe the procedure for conducting inquiries under sections 59 and 63 of the Financial Management and Audit Act 1990; and

(c) prescribe the maximum amount that may be written off by a Minister or Head of Agency.

18.7 Limitation Act 1974

The Limitation Act 1974 stipulates time frames information is required to be kept for the purpose of actions and arbitration. These may relate to actions in respect of personal injuries incurred before or after commencement day, claims in equity, adverse possession of land, rent recovery disability, fraud and mistake and repeals.

18.8 Personal Information Protection Act 2004

The Personal Information Protection Act 2004 specifies the minimum legal requirements for collecting, using and protecting a record, as well as confidentiality. Schedule 1 of the Act contains the 10 Personal Information Protection Principles (PIPP):
15. Collection
16. Use and Discloser
17. Data Quality
18. Data Security
19. Openness
20. Access and Correction
21. Unique identifiers
22. Anonymity
23. Disclosure of information outside Tasmania
24. Sensitive information

These principles stipulate that personal information held by an organisation is:

- accurate, complete, up to date, and relevant to its functions and activities (PIPP 3), (PIPP 6)
- used only for a purpose in which it is relevant, and only for the purpose for which it obtained, unless an exemption is applicable (PIPP2)
- to take reasonable steps to protect the information it holds from misuse, loss, unauthorised access, modification or disclosure (PIPP4), (PIPP 9).

18.9 Right to Information Act 2009


The object of the Right to Information Act is to improve democratic government in Tasmania by increasing the accountability of the executive to the people of Tasmania, and increasing the ability of the people of Tasmania to participate in their governance by acknowledging that information collected by public authorities is collected for and on behalf of the people of Tasmania, and is the property of the State.

This object is to be pursued by giving members of the public the right to obtain information held by public authorities and Ministers, and by giving members of the public the right to obtain information about the operations of Government.

As a public authority, the University of Tasmania is bound by the provisions of the Right to Information Act and is committed to furthering the objects stated within it.

18.9.1 Section 11 – Information held by Archives Office

1. A record placed in the custody of the Archives Office by a public authority is taken for the purposes of this Act to be information in the possession of that public authority or, if that public authority no longer exists, the public authority the functions of which the information is most closely related to.
2. Notwithstanding subsection (1), records of a Royal Commission or a Commission under the Commissions of Inquiry Act 1995 deposited in the Archives Office are, for the purpose of this Act, to be taken to be information in the possession of the Department.
3. Subsection (1) does not apply to a record that can be inspected by the public at the Archives Office otherwise than in accordance with this Act.
4. Sections 15 and 16 of the Archives Act 1983 do not prevent a person from being provided, in accordance with this Act, with information contained in a State record deposited in the Archives Office.
5. This Act does not affect access to records in the Archives Office in accordance with the Archives Act 1983.

Work Health and Safety Act - Section 276 Legislative making Powers – Schedule 3.6
Records and Notices is the enabling legislation with regard to Work Health and Safety recordkeeping.

The recordkeeping requirements of the Act are documented in the Regulations including:

- S 50 Monitoring airborne contaminants
- S 76 Confined Spaces – records of training
- S237 Records of plant
- S378 Hazardous chemicals – health monitoring records
- S388 prohibited and restricted carcinogens – health monitoring records
- Lead – health monitoring records
- S444 Asbestos – health monitoring records
- Table 14.i Hazardous chemicals requiring health monitoring
Appendix II - Recommended storage media for physical/paper records

- File covers should be made of quality heavyweight manila board in white or buff. The recommended size is 388 x 240mm and use of reinforced colour tabs is recommended to identify the originating area/division/section.
- Tabs, lateral file fasteners and tubeclips/mediclips make viewing, adding, removing and photocopying contents of the file easier.
- Alpha-numeric colour coded labels help identify misfiles if and when they occur.
- Out-guides help keep track of files and hold loose papers for when the file is returned.
- File/toaster racks support files to keep them upright and together in the file cabinet.
- Storing records in open bays or lockable lateral shelving units is recommended where possible.
- Permanent records will need to be placed in Type 1 (17x25x38cm) acid-free archival boxes (blue/grey in colour) and metal clips and fastenings removed to reduce rust issues.
- Temporary records can be kept in Type 1 (17x25x38cm) craft board boxes (brown) or standard commercial document storage providers' boxes.