FOREWORD

Murdoch University has a continuing commitment to the delivery and management of quality recordkeeping practices to meet its operational business needs, accountability requirements and the expectations of the community.

In accordance with the State Records Act 2000 I endorse the Procedures Manual of the Records Management & Archives Office. The manual is intended to demonstrate adherence to the legislative, industry best-practice and related recordkeeping practices observed by the University.

Trudi McGlade
University Secretary
Murdoch University

Date:
## CONTENTS

<table>
<thead>
<tr>
<th>Organisation Chart</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>7</td>
</tr>
<tr>
<td>1.1 What is a Record?</td>
<td>7</td>
</tr>
<tr>
<td>1.2 What is Records Management?</td>
<td>8</td>
</tr>
<tr>
<td>1.3 What is a Recordkeeping System?</td>
<td>8</td>
</tr>
<tr>
<td>1.4 Why Records must be Managed</td>
<td>8</td>
</tr>
<tr>
<td>1.5 Stakeholders</td>
<td>9</td>
</tr>
<tr>
<td>1.6 Responsible Officer</td>
<td>10</td>
</tr>
<tr>
<td>1.7 Role of the Records Management &amp; Archives Office</td>
<td>10</td>
</tr>
<tr>
<td>1.8 Key Performance Indicators</td>
<td>11</td>
</tr>
<tr>
<td>1.9 Professional Development</td>
<td>11</td>
</tr>
<tr>
<td>1.10 Budget and Procurement</td>
<td>13</td>
</tr>
<tr>
<td>1.11 Annual Report</td>
<td>13</td>
</tr>
<tr>
<td>2. Legislation</td>
<td>14</td>
</tr>
<tr>
<td>2.1 Introduction</td>
<td>14</td>
</tr>
<tr>
<td>2.2 State Records Act 2000</td>
<td>14</td>
</tr>
<tr>
<td>2.3 Freedom of Information Act 1992</td>
<td>15</td>
</tr>
<tr>
<td>2.4 Evidence Act 1906 and Acts Amendment (Evidence) Act 2000</td>
<td>16</td>
</tr>
<tr>
<td>2.5 Parliamentary Commissioner Act 1971</td>
<td>16</td>
</tr>
<tr>
<td>2.6 Criminal Code Act 1913</td>
<td>17</td>
</tr>
<tr>
<td>2.7 Electronic Transactions Act 2003</td>
<td>18</td>
</tr>
<tr>
<td>2.8 Financial Management Act 2006</td>
<td>18</td>
</tr>
<tr>
<td>2.9 Auditor General Act 2006</td>
<td>18</td>
</tr>
<tr>
<td>2.10 Privacy Amendment (Private Sector) Act 2000</td>
<td>19</td>
</tr>
<tr>
<td>3. Records Management System HP-TRIM</td>
<td>20</td>
</tr>
<tr>
<td>3.1 Background</td>
<td>20</td>
</tr>
<tr>
<td>3.1.1 Security of Records</td>
<td>20</td>
</tr>
<tr>
<td>3.2 Support Information Databases</td>
<td>21</td>
</tr>
<tr>
<td>3.2.1 Central Files Locator</td>
<td>21</td>
</tr>
<tr>
<td>3.2.2 Senate Minutes Database</td>
<td>21</td>
</tr>
<tr>
<td>3.2.3 Academic Council Minutes Database</td>
<td>21</td>
</tr>
<tr>
<td>3.2.4 University Publications Database</td>
<td>22</td>
</tr>
<tr>
<td>3.2.5 Resources Committee Minutes Database</td>
<td>22</td>
</tr>
<tr>
<td>4. Responsibility to Create and Keep Records</td>
<td>23</td>
</tr>
<tr>
<td>4.1 Introduction</td>
<td>23</td>
</tr>
<tr>
<td>4.2 Corporate Records</td>
<td>23</td>
</tr>
<tr>
<td>4.3 Ephemeral Records</td>
<td>24</td>
</tr>
<tr>
<td>4.4 Personal Records</td>
<td>25</td>
</tr>
<tr>
<td>4.5 Drafts, Copies, and Working Papers</td>
<td>26</td>
</tr>
<tr>
<td>4.6 Audiovisual Records</td>
<td>26</td>
</tr>
<tr>
<td>4.7 Photographic Records</td>
<td>27</td>
</tr>
</tbody>
</table>
4.8 Records Relating to Aboriginal People ................................................................. 28
4.9 Research Institutes and Centres ......................................................................... 29
4.10 Records Received from Offices and Schools .................................................. 29
  4.10.1 University Secretary’s Office ........................................................................ 30
  4.10.2 People and Culture Office .......................................................................... 30
  4.10.3 Admissions and Recruitment Support ...................................................... 31
  4.10.4 Research Ethics Office ................................................................................ 31
  4.10.5 Education, Curriculum and Academic Policy ........................................... 32
4.11 Statutes and By-Laws ....................................................................................... 32
4.12 Recordkeeping Training Program .................................................................... 32
  4.12.1 Online Recordkeeping Training Course .................................................... 32
  4.12.2 Why Online Training? .............................................................................. 33
  4.12.3 Purpose of the Training Program ............................................................. 33
  4.12.4 Management of the Training Course ....................................................... 33
  4.12.5 Survey Tool ............................................................................................... 34

5. Security, Confidentiality and Privacy .................................................................. 35
  5.1 Security ............................................................................................................. 35
  5.2 Confidentiality .................................................................................................. 36
  5.3 Privacy .............................................................................................................. 38

6. Access to Records ............................................................................................... 40
  6.1 Access Guidelines ............................................................................................ 40
  6.2 Public Access to Records ................................................................................. 41

7. File Titling, Classifying and Filing ...................................................................... 42
  7.1 Classification System ....................................................................................... 42
  7.2 Classifying Correspondence ............................................................................ 43
  7.3 Filing of Correspondence ................................................................................. 44
  7.4 Indexes ............................................................................................................. 44
  7.5 Shelf Collection ................................................................................................ 44

8. Central Files ....................................................................................................... 45
  8.1 Arrangement of Files ....................................................................................... 45
  8.2 Borrowing Central Files .................................................................................. 45
  8.3 How long Can a File be Loaned? ..................................................................... 46
  8.4 Returning Files to the Records Management Office ....................................... 46
  8.5 Transferring Files ............................................................................................ 46
  8.6 Taking Central Files off Campus ...................................................................... 47
  8.7 Confidential Files .............................................................................................. 47
  8.8 Booking Files (Bring-Forward entries) .............................................................. 47
  8.9 Requesting a New File to be created ............................................................... 48
  8.10 File Creation Procedures ................................................................................ 48
  8.11 Closure of Files ............................................................................................... 49
  8.12 Lost Files ........................................................................................................ 50
  8.13 Annual Review, Cull and Disposal ................................................................. 50

9. Committees ....................................................................................................... 51
  9.1 Recordkeeping Requirements .......................................................................... 51
  9.2 External Committees ....................................................................................... 52
15. **Retention and Disposal** ................................................................. 82
   15.1 Overview .................................................................................. 82
   15.2 Disposal Authorities ................................................................ 82
   15.3 Disposal of Records ................................................................. 83
   15.4 Authority to Destroy Records .................................................. 83
   15.5 Copies of Records ...................................................................... 83
   15.6 Draft Documents and Working Papers ...................................... 84
   15.7 Ephemeral Records .................................................................... 84
   15.8 Freedom of Information, Litigation, Investigations, and Audits ... 84
   15.9 Procedures for the Disposal of Records ..................................... 84
   15.10 Scope of Disposal Authorities .................................................. 85
   15.11 Penalties ..................................................................................... 86
   15.12 Review ...................................................................................... 86

16. **Archival Records** ...................................................................... 87
   16.1 Role of the Murdoch University Archives .................................. 87
   16.2 State Archives .............................................................................. 87
   16.3 Responsibilities ........................................................................... 88
   16.4 Acquisition and Appraisal ........................................................ 88
   16.5 Collection Policy ......................................................................... 89
   16.6 Access and Control ...................................................................... 91

17. **Murdoch University History** ................................................... 93
   17.1 Research and Promotion .......................................................... 93
   17.2 Murdoch University History Collection Advisory Group ........ 94

18. **Offsite Storage of Temporary Records** ..................................... 95
   18.1 Introduction ................................................................................ 95
   18.2 Numbering System .................................................................... 95
   18.3 Receiving Records from Offices and Schools ........................... 95
   18.4 Preparing Cartons for Transfer to Storage ................................. 96
   18.5 Retrieving Cartons from Storage .............................................. 97
   18.6 Permanent Retrieval of Cartons .............................................. 98
   18.7 Amending an Existing Work Order .......................................... 98
   18.8 When a Requested Carton is Delivered .................................... 98
   18.9 Returning Cartons to Storage .................................................. 98
   18.10 Ordering New Cartons ............................................................. 98
   18.11 Cost Centres ............................................................................. 99
   18.12 Destruction of Cartons ............................................................. 100
   18.13 Invoicing .................................................................................... 100
1. **Introduction**

As a State organisation, Murdoch University is subject to the *State Records Act 2000 (WA)*. The primary intention of this Act is to strengthen organisational accountability and transparency in State and Local Government organisations in Western Australia by regulating the creation, retention and disposal of records. The Act emphasises the responsibility of all staff to ensure the systematic creation of proper and adequate records of the University’s business activity and their inclusion in appropriate recordkeeping systems and eventual disposal of the records.

The systematic creation and capture of records into the University’s recordkeeping systems is fundamental to the efficient and effective functioning of university administrative processes. Quality recordkeeping practices underpin decision-making processes by ensuring the availability and timely access to full and accurate records.

These records must be kept for varying periods of time to ensure they are available to meet administrative needs and as evidence of the University’s activities. They must be disposed only in accordance with officially approved disposal authorities, thereby protecting the University from potential administrative or legal issues.

The proper management of records is also essential in upholding the University’s reputation as a transparent and accountable public institution. It ensures the University can satisfy the scrutiny of parliament and the Auditor General and meet community expectations. In addition, it allows the University to meet official requests for records by the FOI Commissioner and the State Ombudsman among others.

Proper and adequate records may also be needed as prima facie evidence to support the University’s defence of its decision-making processes during litigation, or be required by legal processes such as discovery orders and subpoena. An inability to provide records that substantiate the University’s activities may be seen as a major failure in organisational accountability.

This manual sets out the procedures and practices that are currently in place at Murdoch University in relation to the management of its records by the Records Management & Archives Office.

1.1 **What is a Record?**

The International Standard on ‘Information and Documentation – Records Management (ISO 15489-1:2001)’ defines a record as “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”.

The *State Records Act 2000* provides a detailed explanation about what is included in the definition of a record. Consequently, a ‘record’ is any record of information however recorded including:
(a) Any thing on which there is writing or Braille
(b) A map, plan, diagram or graph
(c) A drawing, pictorial or graphic work, or photograph
(d) Any thing on which there are figures, marks, perforations, or symbols, having a meaning for persons qualified to interpret them
(e) Anything from which images, sounds or writings can be reproduced with or without the aid of anything else
(f) Any thing on which information has been stored or recorded, either mechanically, magnetically, or electronically

Therefore, information recorded in any medium or form including correspondence, spreadsheets, e-mail, databases, content on websites, plans, publications, photographs, registers, diaries, film and maps are a record and, as such, must be maintained as evidence of the University’s business activities and the conduct of its affairs.

1.2 What is Records Management?

Records Management is a logical and organised approach to the management of information throughout its life cycle, from the point of creation to its eventual disposition. This includes identifying, classifying, storing, protecting, access and use, and the eventual destruction or permanent preservation of records.

Records Management enables the University to control the quality and quantity of information that it creates and receives, and ensures it is able to meet the requirements of its regulatory environment. Records are kept as evidence of the University’s activities, transactions and decisions and form what is commonly called the ‘corporate memory’ of an organisation.

1.3 What is a Recordkeeping system?

A recordkeeping system is an information system that captures, maintains, and provides authorised access to records over time. A recordkeeping system may be paper-based or electronic. The University currently uses HP TRIM to manage its physical records.

The University also maintains numerous business information systems to manage key activities including student records, human resource functions, financial transactions, academic research, and teaching and learning records.

1.4 Why Records must be managed

The proper management of the University’s records underpins business processes and administrative efficiencies, and is essential if the University is to uphold its reputation as a transparent and accountable public institution. Apart from the routine day-to-day needs of staff, the requirement to responsibly manage records is evidenced by the crucial role that records play when they are needed to protect the University’s interests during
litigation, and when they are required by internal and external audits, investigations and reviews.

Numerous benefits accrue to the University by embracing best practice records management practices. These include:

- underpins organisational accountability by ensuring the University’s processes can stand up to public scrutiny;
- provides evidence of responsibility for management’s decision-making;
- promotes administrative efficiencies by ensuring that staff have timely access to relevant and complete records;
- promotes informed decision-making;
- prevents the illegal, arbitrary and premature destruction of records, thereby protecting the University’s corporate memory and ensuring it is kept available for future reference;
- ensures that records are available and easily located when needed to protect and support the University when defending or taking legal action;
- facilitates finding records requested through legal processes such as discovery orders and subpoenas, Freedom of Information applications, or required by the Auditor General and other external agencies;
- protects the interests of the University’s stakeholders including its students, staff, government agencies, research funding organisations, business entities, and the public;
- better protects vital records that establish and protect the legal and financial rights and interests of the University and of its employees and clients;
- ensures that State archives are identified and protected as an important contribution to the State’s cultural heritage;
- facilitates compliance with other legislation;
- expedites continuity whenever staff movements occur.

1.5 Stakeholders

The University is accountable to many stakeholders with an interest in the effective and efficient management of its records. Its major stakeholders are:

- Australian Government (funding by) through the Department of Education and Training (Commonwealth)
- Courts, The
- Employees
- Entities that do business with Murdoch University
- Government agencies (WA) including the Auditor General, FOI Commissioner and Ombudsman
1.6 **Responsible Officer**

As the chief executive officer of the University the Vice Chancellor\(^1\) is responsible for ensuring the University’s compliance with the requirements of the *State Records Act 2000*. This responsibility is delegated to the Manager, Records Management & Archives.

Responsibility for the Murdoch University records management and archival program lies with the Records Management & Archives Office. The Manager, Records Management & Archives reports to the University Secretary who heads the University Secretary’s Office.

1.7 **Role of the Records Management & Archives Office**

The role of the Records Management & Archives Office is to manage the records of the University throughout their life cycle, from creation to eventual disposition, and to ensure that accountability standards with respect to university records are met. This requires the development of policies, guidelines, procedures, the implementation of records and information management systems, and a training program.

The objectives of the Records Management & Archives Office are:

- support administrative processes by ensuring that requirements to create, manage and make accessible full and accurate records of the University’s business activities are met;
- improve the availability and accessibility of information;
- ensure the University meets public accountability requirements including scrutiny by Parliament and the Auditor General;

---

\(^1\) *State Records Act 2000* s.10(1), *Financial Administration and Audit Act 1985* s.52(2), and *Murdoch University Act 1973-1985* s.23(1)
● ensure the University’s compliance with legislative requirements, in particular the *State Records Act 2000*, and best practice standards;
● develop, implement and review the University’s Recordkeeping Plan including policies, procedures, guidelines, disposal authorities and other requirements of the *State Records Act 2000*;
● administer the University Archives;
● promote a culture of quality recordkeeping practices throughout the University;
● provide a recordkeeping training programme to facilitate staff compliance with university policy and the requirements of the *State Records Act 2000*;
● Manage risk issues.

### 1.8 Key Performance Indicators

The Records Management & Archives Office will periodically revise and update its key performance indicators. The purpose of the KPIs is to help the Office define and measure its progress towards key goals and align the focus of its work with the University’s overall strategic direction. The following performance indicators have been developed to measure the efficiency and effectiveness of the University’s recordkeeping systems:

- Provision of quarterly statistical information for senior management including the number of new hardcopy records registered in the recordkeeping system, the number of cartons of records transferred to storage, the number of cartons of records destroyed, and the number of staff to have completed the recordkeeping awareness training course;
- When an EDRMS is implemented, the following performance indicators will be used to assess the degree to which the system is successfully meeting objectives and for gauging staff satisfaction with the system:
  - Number of new records registered
  - Number of new users registering documents
  - Percentage of users finding correct records
  - Number of issues/incidents reported and resolved (system technical reliability)
  - Percentage of users satisfied with the system
  - Quality assurance processes to review the integrity and accuracy of data

### 1.9 Professional Development

Murdoch University has an active commitment to the ongoing professional development and training of its academic and professional staff. Given the dynamic nature of the records and information management profession, Records Management & Archives staff are encouraged to utilise opportunities for professional development and training.
Professional development funding is allocated directly to the Schools and Offices. The University Secretary has overall responsibility for the use and authorisation of funds in the University Secretary’s Office.

The Organisational Capability Unit (within the People and Culture Office) has responsibility for the University’s internal training and staff development program. OCU offer professional development programs for all staff including face-to-face and online training programs.

The Murdoch e-Learning Platform (MeLP) utilises the ELMO learning management system. This system provides staff with a large range of online training courses, some of which require mandatory completion. Staff are able to self-enrol in the training courses. Completion of training is automatically recorded at the MyTraining website for staff and supervisor reference purposes.

Completion of a select number of training courses is considered mandatory for all staff. These courses are termed ‘compliance e-learning training courses’ and include the Recordkeeping Awareness Training Course – refer 4.12 Recordkeeping Training Program. Newly commencing staff are required to complete the compliance training courses as part of their induction and during their 3-month probation period. Existing staff are required to undertake refresher training for the compliance modules every two years.

The University encourages and funds staff attendance at conferences, workshops, seminars, lectures and training courses organised through external training providers and professional associations. In relation to records management training needs, the following organisations provide training, consulting, and recruitment services in the records and information management fields:


External training providers can be utilised for specialised training needs such as business writing skills, communication and interpersonal skills, project management, IT training, and health and wellness programs where these aren’t satisfactorily covered by the University’s professional development program. The following external training provider is widely used by the University:


Every 3-4 years, the University generously supports the Records Manager & Archivist’s attendance at the annual Inforum-RIMPA information and records management convention. Attendance is invaluable for keeping abreast of current developments and challenges in the records management profession and for developing networking opportunities.
1.10 Budget and Procurement

The Finance Office has responsibility for developing the University’s annual budget. It is a complex undertaking that incorporates Government funding, government policy, the financial implications of higher education reform, estimates of student load, tuition fees, strategic priorities, capital projects, salary growth, planned investment income, provision for extraordinary items, and operational costs. Considerations about the long-term financial sustainability of the University guide and influence the budget process.

The University Secretary has responsibility for the budget of the University Secretary’s Office. Provision for standard expenditure items such as salaries, offsite storage fees, and stationery do not require input from the Records Management & Archives Office. However, requests for non-routine expenditure items such as conference attendance, new furniture and shelving require a written submission including appropriate detail and justification.

All procurement activities are required to comply with the University’s Procurement Policy and the attendant Procurement Procedure. This policy framework has a number of core principles that underpin the procurement process including an obligation to ensure value for money and to ensure that university funds are used efficiently and effectively.

Staff are required to use a Nominated Supplier where such arrangements have been negotiated for operationally strategic items. A list of nominated suppliers is available at the Procurement webpage.

A formal procurement process, involving a tender process, is required where the value of goods and services is in excess of $100,000.

1.11 Annual Report

Each year, in accordance with Standard 2 Principle 6 ‘Recordkeeping Plans – Compliance’ issued under s.61 of the State Records Act 2000, the University is required to provide in its Annual Report a brief report on its strategies for ensuring staff compliance with the recordkeeping plan. The Manager Records Management & Archives has responsibility for preparing the report. The University Secretary will review the report and, where required, make amendments before authorising its publication in the Annual Report.

The Standard requires the following compliance requirements to be addressed:

- Evaluate the efficiency and effectiveness of the University’s recordkeeping systems at least once every five years;
- Conduct a recordkeeping training program and periodically review its efficiency and effectiveness;
- Ensure that employee roles and responsibilities concerning their compliance with the recordkeeping plan are addressed by the University’s induction program.
2. Legislation

2.1 Introduction

Murdoch University was established under Statute and is therefore accountable to the Parliament of Western Australia and any relevant Commonwealth and State legislation. The principal legislation governing records management in WA is the State Records Act 2000. A summary of the Act’s main provisions, as well as key records management references found in other legislation, is provided below.

2.2 State Records Act 2000

The State Records Act 2000 (WA) governs the way the University must manage its records. All ‘State organisations’ are covered by the Act including public sector agencies, universities, TAFE institutes, parliamentary departments, local government, and Royal Commissions.

The primary intention of the Act is to strengthen organisational accountability and transparency in the recordkeeping practices of State and Local Government agencies through the implementation of effective record keeping practices.

The operation of, and compliance with, the Act is monitored by the State Records Office and the State Records Commission, the latter having authority to enquire into any breaches or possible breaches of the Act.

Key provisions of the State Records Act 2000 include:

- The University is required to have a ‘recordkeeping plan’, approved by the State Records Commission. The recordkeeping plan consists of a series of documents relating to the University’s recordkeeping systems, retention and disposal arrangements, policies, practices and processes;
- All employees of the University, and contractors and consultants providing services to or on behalf of the University, have a legal responsibility to create records that sufficiently record the performance of the University’s functions;
- The destruction of the University’s records must be in accordance with approved retention and disposal authorities;
- The University is responsible for preservation strategies to ensure its records are protected and preserved for the duration of their retention requirements;
- The University must conduct a recordkeeping training program;
- Offences – there are penalties for non-compliance with the Act, including a failure to create and keep proper and adequate records; unlawful transfer of a record; and destruction of records other than in accordance with an approved disposal authority;
A ‘State Records Commission’ was established under the terms of Part 8 of the State Records Act 2000. Membership consists of the Auditor General, Information Commissioner, the State Ombudsman, and the Governor’s Appointee. The SRC has responsibility for producing standards and principles to govern key aspects of recordkeeping in government organisations;

To-date, the following Standards have been developed by the State Records Commission:

- SRC Standard 1: Government Recordkeeping
- SRC Standard 2: Recordkeeping Plans
- SRC Standard 3: Appraisal of Records
- SRC Standard 4: Restricted Access Archives
- SRC Standard 5: rescinded
- SRC Standard 6: Outsourcing
- SRC Standard 7: State Archives Retained by Government Organisations
- SRC Standard 8: Managing Digital Information

2.3 Freedom of Information Act 1992

The Freedom of Information Act 1992 provides for public access to documents held by the University, and to enable the public to ensure that personal information held by the University about them is accurate, complete, and up-to-date and not misleading.

- **Definition of a record** - The definition of a record in the FOI Act is very broad and includes documents, maps, plans, drawings, diagrams, photographs, any thing from which sounds, images or writing can be reproduced, and any article on which information has been stored or recorded either electronically, mechanically or magnetically. All university records, regardless of the media they are created in, are subject to disclosure under this Act;

- **Exempted records** - A range of documentation is exempted from disclosure under the Act. The exemptions are strictly defined and are severely limited by the need to prove that disclosure would be against the public interest, except in the case of the exemption that concerns legal professional privilege;

- **Preservation** - Once a request for access under the FOI Act has been lodged all records relevant to that request, regardless of whether they are due for destruction, must be identified and preserved until action on the request and on any subsequent internal and external reviews are completed;

- **Publicly available documents** – The access procedures covered by the FOI Act do not apply to documents that are available for purchase or free distribution. Examples include the annual report, Handbook, student prospectus, academic transcripts, agendas and minutes of most committees, examination scripts, internal manuals and publications of the University;

- **Offences** - A staff member that conceals, destroys or disposes of a document or part of a document or refuses to comply with a request to provide access to a document, commits an offence under the Act and is liable to a fine of $6,000;
Failure to disclose all documents may be construed as a deliberate attempt to hide documents from public scrutiny and hence constitute a breach of the University’s obligations under the Act;

- The Records Management & Archives Office creates central files for all new Freedom of Information requests. All FOI files are confidential and have restricted access.

2.4 Evidence Act 1906 and Acts Amendment (Evidence) Act 2000

- Records provide evidence of the University’s business activities, transactions and decisions;
- The Act provides for documents to be subpoenaed for litigation purposes;
- The law of evidence requires documents to be authentic, complete and accurate if they are to be admissible in a court of law;

A court of law may need to establish that a record is what it claims to be, it was created by the person who claims to have created it, the record was created at the time claimed, and the record has not been altered by an unauthorised officer. The quality and integrity of the University’s recordkeeping processes is therefore paramount;

- The Act’s definition of a document is very broad. It includes documents, books, maps, plans, photographs, discs, and tapes;
- The Act provides for a court of law to direct any document received in evidence to be impounded and kept in the custody of the court until further order;
- The Act contains various provisions concerning the reproduction of documents as admissible evidence before a court of law;
- Any microfilming arranged by university Offices must be produced in accordance with the requirements of the Evidence Act 1906, in particular the admissibility of reproductions as evidence. The best evidence rule permits micrographic reproductions of documents to be accepted where the original has been destroyed;
- The Act has implications for the destruction of records and the requirements for creating acceptable reproductions;
- The Acts Amendment (Evidence) Act 2000 expands upon the Evidence Act 1906 to permit the admission of evidence created using electronic media.

2.5 Parliamentary Commissioner Act 1971

The Parliamentary Commissioner for Administrative Investigations (or Ombudsman) investigates complaints from the public about Western Australian State Government agencies, statutory authorities, local governments and public universities.

There are certain conditions that must be satisfied before the Ombudsman will investigate a complaint made against the University. These are:
● It must relate to a matter of administration. That is, complaints about actions and decisions of the University to see if they are wrong, unjust, unlawful, discriminatory or unfair;

● It must affect the complainant personally. Hence, nearly all complaints originate from the University’s staff and students;

● The Ombudsman will not investigate a complaint until it has first been raised with the University by the complainant and has gone through the University’s internal complaints processes.

To assist in the investigation of a complaint the legislation grants the Ombudsman authority to request any documents or records from the University that will be relevant to the investigation. When investigating any matter the Ombudsman has all the powers and rights specified in the Royal Commissions Act 1968 as applying to a Royal Commission and its Chair.

The ability of the University to comply efficiently and effectively with the requirements of the Act is dependent upon the quality of its administrative practices, in particular its records management processes and practices.

The Records Management & Archives Office maintains files for all Ombudsman complaints.

2.6 Criminal Code Act 1913

Western Australia’s Criminal Code Act is a comprehensive codification of criminal law and the primary instrument for the source of criminal law in WA. Key provisions of the Act concern the falsification of records, destruction of evidence, and forgery of records. Penalties recognise the seriousness of offences and include up to seven years imprisonment and substantial fines.

The main provisions of the Act concerning the keeping of records are:

● **Falsification of records by a public officer**
  Any public officer who, in the performance or discharge of the functions of their office or employment, corruptly
  (i) makes any false entry in any record;
  (ii) omits to make any entry in any record;
  (iii) by act or omission falsifies, destroys, alters or damages any record; is guilty of a crime and is liable to imprisonment for 7 years.

● **Destroying evidence**
  Any officer of the University who, knowing that any record is or may be required in evidence in a judicial proceeding, wilfully destroys it or renders it illegible or undecipherable or incapable of identification, with intent thereby to prevent it from being used in evidence, is guilty of a crime, and is liable to imprisonment for 7 years.
• Forgery and uttering
  Any officer of the University who with intent to defraud forges a record; or utters a
  forged record, is guilty of a crime and is liable to imprisonment for 7 years.

2.7 Electronic Transactions Act 2003
This Act gives legal recognition to transactions that take place wholly or partly by
electronic communications. The intention of the Act is to provide a legal and regulatory
framework that:
  • Recognises the importance of electronic communications;
  • Facilitates the use of electronic communication as a way of entering into
    transactions;
  • Promotes business and community confidence in the use of electronic
    communication as a way of entering into transactions; and
  • Enables business and the community to use electronic communication in their
    dealings with government.

Information is defined by the Act to include any information in the form of data, text,
images or sound.

The Act contains a number of provisions concerning the recording of information in
electronic form. These include:
  • electronic signatures;
  • retention of documents on a data storage device;
  • retention requirements;
  • accessibility of documents stored electronically;
  • maintenance of the integrity of the electronic information.

2.8 Financial Management Act 2006
The Financial Management Act 2006 and associated Treasurers Instructions provide for the
management, administration and reporting of the finances of State public agencies.

Although the Act contains only limited references to records management functions
there, nevertheless, is an implicit expectation that effective records management
processes and procedures are essential to ensuring the proper management, access and
maintenance of financial and accounting records.

2.9 Auditor General Act 2006
  • The key function of the Auditor General is to examine, investigate, inspect and
    review an agency’s accounts and financial statements;
The functions of the Auditor General also include responsibility for examining an agency's compliance with legislative provisions, public sector policies and its own internal policies;

For purposes of an audit the Auditor General is entitled to full and free access at all reasonable times to the records of the University. These include all accounts, information, documents, books, writings, monetary forms, vouchers, systems and records that the Auditor General considers to be relevant to its audit of the University's activities.

2.10 Privacy Amendment (Private Sector) Act 2000

The (Commonwealth) Privacy Amendment (Private Sector) Act 2000 that came into force on 22 December 2001 introduced strict standards for the way in which private sector organisations should manage personal information.

The scope of the Act generally does not include public universities. However, there are limited, but important, exceptions in respect of Tax File Numbers, Medicare Numbers and obligations under the Higher Education Support Act 2003 (HESA) in the way the University manages personal information.

The Higher Education Support Act requires higher education providers to comply with the Australian Privacy Principles (APPs) set out in the Privacy Act 1988 as amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 in relation to students' personal information collected for the purposes of section 36-20 Chapter 3 and Chapter 4 of the HESA.

Accordingly, the University’s Privacy Policy has incorporated the Australian Privacy Principles and includes comprehensive references in relation to the collection, use and disclosure of personal information.
3. Records Management System HP-TRIM

3.1 Background

Hewlett Packard (HP) TRIM is the records management system used by the Records Management & Archives Office. TRIM was implemented in 1999 following a formal evaluative and approval process, and in accord with the University’s Strategic and Quality Improvement Pan (1997-2002). SQIP Objective M.3 included an operational strategy encouraging the implementation of strategic computer systems that provided the best possible storage, access and retrieval of the University’s information.

HP-TRIM provides the Records Management & Archives Office with a sophisticated database for capturing, managing and retrieving records. It facilitates effective control over current, intermediate and archival records which can be retrieved using a wide range of search tools. These include relationship-linking capabilities and the ability to search at various metadata levels.

The system design permits a continuum-based approach to the effective management of records from creation/registration date through to the disposal, preservation and use of records as State archives.

The support of barcode technology in HP-TRIM facilitates efficient files census activities and provides the Records Management & Archives Office with tight control over file movements around the University. Barcoding of files also permits efficiencies during the performance of routine tasks such as the transfer of multiple files to archives, offsite storage or to destruction, scanning of multiple files when logging files in and out of the system, assigning multiple records to container locations, and attaching retention schedules to multiple records.

HP-TRIM is currently used for managing physical records.

3.1.1 Security of Records

- Appropriate security and access controls must be assigned to records to protect confidential information from unauthorised access and use. Security levels can be set at the individual record level as well as to entire records series or record aggregations;
- The default for newly registered records is ‘Unclassified’ or ‘General Access’. Confidential records must be assigned a ‘Restricted Access’ classification;
- A typical central file contains a range of documentation. Some of the records will be routine correspondence attracting a ‘General Access’ security classification while some of the records will be of a confidential nature which attracts a ‘Restricted Access’ security classification. In such circumstances the higher classification level must always be assigned to the file.
3.2 Support Information Databases

Records Management & Archives has developed a number of web-based searchable information databases to facilitate the efficient dissemination and access to information. The databases are built on the Oracle Application Express (APEX) development environment and accessed via the Murdoch Authentication and Identification System (MAIS), i.e. via a valid Murdoch username and password.

The databases are available on the University’s intranet at the Records Management & Archives homepage.

The databases are updated by the Records Officer and checked for accuracy and correct formatting by the Records Manager & Archivist.

3.2.1 Central Files Locator

The Central Files Locator provides details of all central administrative files maintained by the Records Management & Archives Office. Access is strictly restricted where the title of a central file contains confidential information, for example, Freedom of Information requests.

This database negates the need for staff in Administrative Offices and the Schools to have access to the TRIM records management system resulting in a considerable budget saving to the University in terms of licence fees.

The Central Files Locator is updated following the creation of new files.

3.2.2 Senate Minutes Database

The Senate has responsibility for establishing the University’s strategic direction, for guiding and approving key policies, delegating authority and accountability, and monitoring and evaluating the University’s performance. The Senate also has a legislative role and has power to make, amend and repeal Statutes, By-laws and Regulations. The Senate bears ultimate accountability for the University. The Senate Minutes Database therefore contains a significant body of important information that can be easily searched by all staff.

The Senate minutes database is updated by Records Management & Archives following receipt of an electronic Word document of the confirmed minutes of the last meeting of Senate.

The database covers all meetings of the Senate from 1973-current.

3.2.3 Academic Council Minutes Database

Academic Council is the University’s senior decision-making body on academic matters. Its responsibilities include academic planning; approval of units, majors and courses of study; reviews of Schools of Study, Institutes and Centres; formulation and approval of
policies and guidelines; establishment and oversight of Centres and Institutes; and development of university legislation.

The Academic Council minutes database is updated by Records Management & Archives following receipt of an electronic Word document of the confirmed minutes of the last meeting of Academic Council.

The database covers all meetings of the Academic Council from 1974-current.

3.2.4 University Publications Database

The ‘Publications’ database provides a summary of articles that have long-term administrative or historic value to the University. These articles appeared in Murdoch University publications such as ‘The Exchange’, ‘In Touch’, ‘Explorer’, ‘Synergy’, ‘On Campus’ and ‘Murdoch News’.

Key articles that are deemed of historical significance and value are selected for inclusion in the database. Summary information of each selected article is entered in the database and includes: the publication, publication date, volume and page number, article headline and a synopsis, keywords, and names of people featured in each article.

The purpose of the database is to make readily available to all staff a useful source of administrative and historical information that would otherwise remain unused and forgotten.

The database covers publications from 1975-current.

3.2.5 Resources Committee Minutes Database

The Resources Committee is an important standing committee of Senate. Its principal functions include review of budgetary and financial matters including those of the University’s trusts and foundations and the finances of the Guild of Students; oversight of the University’s investments; consideration of campus development proposals including the construction of new buildings, road works and car parking facilities.

Access to this database is restricted because of the confidentiality of the committee’s functions. The Vice Chancellor has authorised access to the following officers: Vice Chancellor, Chief Operating Officer, Chief Financial Officer, Director Property and Commercial Services, Chair of the Resources Committee, and Secretary of the Resources Committee.

The database is updated following receipt of the confirmed minutes of the last meeting of the Resources Committee as an electronic format Word document.

The database covers the minutes of the Resources Committee from 1996-current.
4. Responsibility to Create and Keep Records

4.1 Introduction

All Murdoch staff as well as contractors and consultants providing services to, or on behalf of, the University have a responsibility to create proper records that adequately document the performance of the University’s functions.

Records should be adequate to the extent that they allow proper reference to a matter by staff; ensure sufficient evidence is kept of the University’s performance of its functions; and facilitate scrutiny of the University’s activities by external regulatory agencies, in particular the Office of the Auditor General.

A significant volume of the University’s records are generated and maintained by automated processes such as by the accounts payable, student records and payroll systems. Furthermore, records are consistently created as an outcome of normal work processes. For example, a record is created when a purchase order is raised, an email transmission is sent, when committee minutes are written, a database updated, when policies are developed, and when a contract is drafted.

Frequently, however, a conscious decision must be made to create records to ensure that an official record of what was said, done or approved and by whom is made. These circumstances include creating a record of telephone conversations and of the deliberations of meetings particularly when decisions are reached, a course of action agreed upon, and commitments, instructions and authorisations are given.

Staff typically create and receive large numbers of records in the conduct of their work, particularly electronic mail transmissions. However, it is not necessary to capture all such records into a recordkeeping system. There are three types of records that staff should be aware of when determining which records must be captured into a recordkeeping system. These are corporate, ephemeral and personal records.

Refer also the Recordkeeping Guideline for information about staff recordkeeping roles and responsibilities.

4.2 Corporate Records

A corporate record contains information that is relevant to the University’s functions and activities and has continuing value to the University. That is, corporate records are those records that typically relate to the substantive business of the University. Consequently, a corporate record must always be captured into a recordkeeping system. Most records created and received by staff during the performance of their duties are corporate records.

Examples of corporate records include:

- Academic planning, course delivery and teaching and learning records;
• Any record within the definition of a record at 1.1 that adds value or support to an existing record;
• Applications for admission and student accreditation;
• Authorisations for any expenditure;
• Campus/physical planning and development;
• Correspondence with enrolled students, staff, and other organisations;
• Development or amendment of policies, guidelines and procedures;
• Documentation generated by the University’s decision-making bodies including committees, working parties and meetings. Records include agendas, minutes, reports, tabled items and meeting notes;
• File notes of decisions and commitments made in a telephone conversation;
• Information technology project documentation;
• Instructions and authorisations to undertake a specific action or course of action;
• Legal documents including contracts, agreements, memoranda of understandings, leases, and licences;
• Negotiations, commitments and arrangements on behalf of the University;
• Payroll records;
• Personal staff files;
• Reports prepared for external agencies;
• Research data;
• Research project documentation;
• Reviews including organisational, administrative, academic, and 5-yearly School reviews.

The ‘General Disposal Authority for State Government Information’ and the ‘Western Australian University Sector Disposal Authority’ provide extensive listings of corporate records and their retention periods.

### 4.3 Ephemeral Records

An ephemeral record is a record with very short-term value or no value to the University. These records only need to be retained for a very limited period of time (a few hours or days) after which they can be destroyed at any time without reference to the disposal authorities. Ephemeral records can be disposed of once their reference value has ceased and do not need to be captured into a recordkeeping system.

• Advertising and promotional material;
• Advice of meeting arrangements;
• Announcements of social events;
● Audio recordings of committee and other meetings made for the purpose of writing transcripts or minutes and where these have been created;
● Background research;
● Broadcast emails not individually addressed to the recipient and circulated for information or general instruction only;
● Copies and drafts sent only for reference;
● Copies of agendas and minutes;
● Copies of emails where another recipient has responsibility for including the message into the recordkeeping system;
● Copies of emails or documents in personal drives or email folders that have been already included in a records management or business information system;
● Copies of records that have already been captured in the recordkeeping system or an official business information system;
● Copies of records made for personal reference purposes;
● Drafts which do not contain significant or substantive changes or annotations. For example, where only minor edits for grammar and spelling are made;
● Drafts which do not proceed to a final version or where a more complete version exists;
● Duplicate copies of photographs or audio visual records;
● Expired diaries and calendar entries;
● Facilitative records, working notes, calculations and incomplete materials used in the preparation of more substantial drafts or final documents;
● Information received due to membership in a listserv, discussion group or forum;
● Information received or downloaded for information or reference purposes only;
● Magazines and journals received through membership of a professional body;
● Routine or rough calculations;
● Social media and instant messaging communications created for informational or promotional purposes e.g. blogs or tweets;
● Spreadsheets or other documents incorporated into other documents;
● Stationery, furniture and office equipment catalogues;
● Statistics and figures;
● Training course announcements;
● Voice-mail messages once a record of the message has been created.

4.4 Personal Records

A personal record relates to the private affairs of an individual and which has no relevance to the University. Personal records do not need to be captured into a
recordkeeping system. However, where a record incorporates both personal and corporate information as occasionally occurs with email transmissions, the record must be included in a recordkeeping system.

Examples of personal records include arrangements for lunch, emails received from friends and family, medical appointments, non-work related casual communications between staff, and letters or cards of appreciation, sympathy or greetings.

4.5 Drafts, Copies, and Working Papers

Supporting documentation such as drafts, copies, working papers and research notes should be managed according to the following guidelines:

- Generally, when a document has been finalised any previous versions, working papers, rough calculations and background notes can be destroyed once their reference value has ended. These records serve a facilitative purpose and consequently have a temporary usefulness which typically ends once a document has been finalised;
- Drafts and working papers that contain significant information not found in the final version of a document should be retained as official records;
- Exact copies of records can be destroyed at any time;
- Copies of documents that contain significant additional information not shown on the original, such as authorisations and handwritten annotations that elaborate on a matter of some significance, should be retained as official records;
- Copies of documents, such as committee minutes, distributed for information purposes only can be destroyed once their reference value has ceased;
- Working papers relating to the development of University policies and standards should be kept where they provide useful background information;
- Working papers and previous versions of legal agreements, contracts, policies and other significant documentation may be retained where there is a requirement to demonstrate the evolution of a matter and how key decisions were reached.

4.6 Audiovisual Records

Audiovisual records include audio and video tape recordings, compact discs, DVD’s, film and photographs.

The University creates a range of audiovisual records including teaching materials, recordings of graduation ceremonies, coverage of significant public events such as the annual Sir Walter Murdoch Lecture and official opening ceremonies.

Audiovisual records can provide unique information about aspects of the University’s activities in a multi-dimensional format, unlike a record that consists only of textual information. For this reason, some audio-visual records will be retained even where a
textual copy exists. An example is where a transcript of a public lecture is created but where an audiovisual record of the lecture also exists.

Guidelines for the management of audiovisual records:

- Audiovisual teaching materials must be clearly titled and include metadata that identifies the author, unit title, and lecture title;
- Audiovisual records deteriorate in high temperatures and humidity levels and must be maintained in an air-conditioned environment where temperature and humidity levels can be controlled;
- Storage areas that house audiovisual records are to be protected against unauthorised access to safeguard them against loss and accidental or deliberate alteration;
- Disposition activities must be in accordance with authorised disposal schedules. The retention of audiovisual records is determined by a number of factors including:
  - Subject matter of the records
  - Purpose for which they were created
  - On-going use and reference value
  - Possible archival/historical value
- Technological obsolescence is a major risk factor concerning the ongoing useability of audiovisual records. Consequently, these records must be preserved and migrated to new technologies when required to ensure they remain available for use through the duration of their retention requirements.

4.7 Photographic Records

Photographs are deemed to be records within the meaning of the State Records Act 2000 and must therefore be managed in accordance with the Act’s requirements. The following guidelines should be observed in relation to the proper management of photographic images:

- Photographs are to be maintained in an air-conditioned storage environment where temperature and humidity levels can be controlled. They should be kept away from dust and direct light because of the deteriorating effect these elements have on photographic prints, negatives, and slides;
- Photographs must be identifiable. That is, the occasion, place, date and people depicted in images must be identified and catalogued. Identification labels should not be applied directly to photographs;
- Digital photographs should be stored in a suitable repository and managed with appropriate software;
- Photographs should be arranged chronologically or by subject;
- Photographs that depict the University’s mission and activities frequently have ongoing historic value to the University. These records should be identified as State archives, protected, preserved and maintained in a suitable repository;

- Photographs that document insurance issues such as accidents, faulty building construction, chemical spills, wilful damage etc. should be kept for as long as the retention period of the project or claim requires.

Photographs that qualify as State archives must be managed in accordance with ‘SRC Standard 7: State Archives Retained by Government Organisations’. These include images that depict:

- Significant ceremonial events such as the installation ceremonies of chancellors and vice chancellors, inauguration ceremonies, official openings of new buildings, campuses, and Schools of Study, naming ceremonies of lecture theatres, and graduation ceremonies;

- Official events including public lectures, especially the Sir Walter Murdoch and Keith Roby lectures, staff prizes and awards, launch of a new corporate identity;

- Community events such as open days, sporting occasions, and events organised by the Student Guild;

- Students of renown such as Rhodes scholars and guild presidents;

- Senior staff such as chancellors, vice chancellors, professors;

- Official visitors to the University, if significant;

- Development and construction of the University’s campuses, grounds and buildings including lecture theatres, research centres, administrative buildings, and playing fields;

- Aerial photographs that document the development of the University and its grounds;

- Photographs of drawings, maps and models of the University;

- Private developments on campus land such as the St Ives Retirement Village, Murdoch College, student village accommodation, and the Tavern;

- University landmarks such as sculptures and the amphitheatre.

4.8 Records Relating to Aboriginal People

The University is required under section 76 of the State Records Act 2000 to consult with appropriate Aboriginal bodies where records contain information about Aboriginal cultural material, Aboriginal sites or any matter relating to the heritage of Aboriginal Australians. The purpose of the consultation is to determine if the records are to be treated as State archives and, if not, determine an appropriate retention period for the records.
4.9 Research Institutes and Centres

The University’s Research Institutes and Centres maintain the majority of records that they create and receive. However, the following records should be held in the custody of the Records Management & Archives Office.

<table>
<thead>
<tr>
<th>Record Description</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreements in relation to the establishment and operation of Institutes and Centres</td>
<td>Original signed agreements are sent to the Legal Office. After digitisation and inclusion in the LEX database forward to the Records Office</td>
</tr>
<tr>
<td>Annual Financial Statements</td>
<td>Send copy to the Records Office</td>
</tr>
<tr>
<td>Annual Reports</td>
<td>Send copy to the Records Office</td>
</tr>
<tr>
<td>Applications for funding from government schemes</td>
<td>Send copy to the Records Office if application for funding is successful</td>
</tr>
<tr>
<td>Application for additional funding support</td>
<td>Send copy to the Records Office if application for funding is successful</td>
</tr>
<tr>
<td>Business Plans</td>
<td>Send copy to the Records Office</td>
</tr>
<tr>
<td>Committee agendas and minutes</td>
<td>Send copy to the Records Office</td>
</tr>
<tr>
<td>Deeds of Variation</td>
<td>Send original signed agreements to the Legal Office. After digitisation and inclusion in the LEX database forward to the Records Office</td>
</tr>
<tr>
<td>Documentation that indicates how a new Centre or Institute has been established</td>
<td>Send copy to the Records Office</td>
</tr>
<tr>
<td>Evaluations of new Centre and Institute applications</td>
<td>Send copy to the Records Office</td>
</tr>
<tr>
<td>Funding Agreement</td>
<td>Send original signed agreements to the Legal Office. After digitisation and inclusion in the LEX database send to the Records Office</td>
</tr>
<tr>
<td>Joint Venture Agreement</td>
<td>Send original signed agreements to the Legal Office. After digitisation and inclusion in the LEX database forward to the Records Office</td>
</tr>
<tr>
<td>Memoranda of Understanding/Agreement</td>
<td>Send original signed agreements to the Legal Office. After digitisation and inclusion in the LEX database forward to the Records Office</td>
</tr>
</tbody>
</table>

4.10 Records Received from Offices and Schools

The Records Management & Archives Office receives records on a continuous basis from Offices and Schools. The following are a few examples:
4.10.1 University Secretary’s Office

A large percentage of the records created by the University Secretary’s Office contain highly confidential and commercially-sensitive information. Many of these records are covered by ‘Legal Professional Privilege’, a rule of law that seeks to protect confidential communications between legal practitioners and their clients from disclosure. Records include signed original contracts and agreements, legal working (LEX) files, committee minutes and agendas and supporting documentation etc.

The University has specific obligations to the external parties of the contracts and agreements that it signs. The recordkeeping responsibilities in these contracts typically include the requirement to provide secure and proper storage of documents, protection from unauthorised access and disclosure, and the confidential disposal of the records when their retention requirements expire. The Records Management & Archives Office has responsibility for ensuring these requirements are met.

When the University receives a subpoena for documents the Legal Office, with assistance from the Records Management & Archives Office, coordinates the production of the records. Where practicable, all documents must first be copied before being released. They must be retained until the original records have been returned.

Records originating from the University Secretary’s Office are collected daily by the Records Officer. The Records Officer has responsibility for entering details about each record on the TRIM database and ensuring appropriate security protocols are applied. All records require the ‘Restricted Access’ security level. Access to the records is strictly restricted to the University Secretary’s Office.

4.10.2 People and Culture Office

The People and Culture Office undertake regular culls of records and forward them to the Records Management Office for custody and management. These include personal files, workers compensation files, payroll records, salary packaging documentation, training and development records, occupational safety and health, industrial relations, and superannuation records.

People & Culture are required to place records in industry-standard archive cartons supplied by the Records Management & Archives Office and to provide an electronic listing of the records contained in each carton. The description of contents needs to be sufficient to ensure the records can be readily identified via keyword searches and efficiently retrieved if they are requested for loan at a later date.

All records received from the People & Culture Office require the ‘Restricted Access’ security level to be selected in the records management database. Access to records is strictly limited to People & Culture staff according to their delegated authority and ‘need to know’ requirements.

The volume of cartons transferred to Records can occasionally be large and it is therefore necessary for Records staff to ensure sufficient space is available before authorising staff.
to proceed with the transfer of cartons. When a delay in receiving the cartons is necessary, Records staff should advise P&C of an approximate date when the cartons can be transferred.

The Records Officer has responsibility for entering details about the records on the TRIM database and ensuring sufficient detail is provided, applying the appropriate security protocols, and arranging their transfer to storage.

4.10.3 Admissions and Recruitment Support

Hard copy documentation relating to applications for admission to the University is forwarded annually to the Records Management & Archives Office for transfer to offsite storage.

As with 4.10.2 these records comprise a large number of cartons and it is necessary to ensure sufficient space is available in the Records Management Office before the transfer of the records is authorised.

The Admissions and Recruitment Support Office is required to provide an electronic listing of the contents of all cartons being transferred. Generic descriptive information is sufficient for these records. For example, Box 7 ‘Admissions – successful A-D (surnames) - Semester 1, 2018’.

These records contain personal and confidential information and must be assigned a ‘Restricted Access’ security level. They are strictly restricted to staff on a ‘need to know’ basis.

The Records Officer has responsibility for entering details about the records on the TRIM database, ensuring appropriate security protocols are applied, and arranging their transfer to storage.

4.10.4 Research Ethics Office

The Research Ethics Office periodically forward documentation relating to applications for clearance to undertake research project work. The documentation consists of manila folders that hold all documentation relating to a specific research project application and the accompanying documentation and reports of the relevant Animal Ethics Committee or Human Research Ethics Committee.

The Research Ethics Office is required to provide an electronic listing of all individual folders contained in each carton to ensure a complete record of all applications is maintained on the records management system. This ensures the efficient identification of the correct folder and archive carton when the records are requested back from offsite storage.

The Records Officer has responsibility for entering details about each file on the TRIM database, ensuring appropriate security protocols are applied, and arranging their transfer to storage.
4.10.5 Education, Curriculum and Academic Policy

School Academic Policy Coordinators routinely send student appeal files (red folders) and student discipline files (orange folders) to the Records Management Office for custody and maintenance.

The Records Officer has responsibility for entering details about each file on the TRIM database, ensuring appropriate security protocols are applied, and arranging their transfer to storage.

These records contain highly confidential information and access must only be granted to staff with the appropriate delegated authority.

4.11 Statutes and By-Laws

The University occasionally amends its statutes and by-laws. This requires the approval of the University Senate and the Executive Council of the Governor. Once approval has been granted the amendment is published in the Government Gazette under the Education section. The Law Library will photocopy the entry appearing in the Gazette and forward it to the Records Management & Archives Office for placement on the appropriate central file.

4.12 Recordkeeping Training Program

A training program is essential for raising staff awareness of their recordkeeping responsibilities under the *State Records Act 2000* and in raising the overall standard of the University’s recordkeeping. The University is also required by law to manage a recordkeeping training program\(^2\).

4.12.1 Online Recordkeeping Training Course

The Records Management & Archives Office has implemented an online training course as the basis of its training program. The training course is integrated with the ELMO Talent Management suite of training courses administered by the Organisational Development Office.

The Recordkeeping Awareness Training Course addresses staff responsibilities under the *State Records Act 2000* including the creation, capture, access, and disposal of records, confidentiality and privacy issues, and security considerations.

A 3-point escalation process has been implemented to ensure that staff undertake the training. The training course is promoted at senior management level, and regular reminders are provided in the staff announcements communication tool.

Refresher training for the compliance modules is required for all staff every two years.

\(^2\)State Records Commission Standard 2 Principle 6 Recordkeeping Plans - Compliance
The Records Manager is required to review and update the training course on an annual basis, and to provide quarterly and annual statistics of staff completion numbers to the University Secretary.

4.12.2 Why Online Training?

An online training approach was chosen for the following reasons:

- Cost Effectiveness: The cost of sending large numbers of staff to attend externally-run training courses is significant. The per-person cost of an online training course is considerably less and delivers substantial volume savings;
- Accessibility and convenience: The online training course provides staff with considerable flexibility with regards to work and time commitments:
  - It can be accessed 24/7
  - It is accessible directly from the desktop
  - The course does not need to be completed in one sitting but continues at the point where staff last logged out
  - It is time efficient. Staff are not required to travel to attend a training course but can train in their own office at their own pace and according to their work schedules
- An online training course allows a broader range of content to be covered than in a classroom setting;
- Research suggests that online training has a higher learning retention rate than courses taught in a classroom environment;
- Availability of refresher training. Upon completion of the training course, staff thereafter may log into the course at any time and review the entire course or selected components of the course.

4.12.3 Purpose of the Training Program

The training program serves three principle aims. These are:

- Promote the benefits of managing records according to best practice principles;
- Raise staff awareness of their responsibilities under the State Records Act 2000 and other applicable legislation; and
- Raise the overall standard of recordkeeping at the University.

4.12.4 Management of the Training Course

- The training course is customisable and allows amendments to the content;
- A direct broadband connection with Telstra allows many concurrent users;
- Upload of data (new staff details) is performed monthly via a system-generated script;
A system-generated email is sent to new staff advising of their enrolment in the training course as part of their induction;

Murdoch University has full access to all data and owns the data;

A range of reporting functions are available;

Any issues should be managed in liaison with the Organisational Development Office.

4.12.5 Survey Tool

A survey tool provides an opportunity for staff to provide feedback about the Recordkeeping training course.

A system-generated email is sent to staff upon successful completion of the training course assessment encouraging them to complete a short survey;

Completion of the survey is optional;

The survey data provides useful information about the effectiveness of the training course in transmitting knowledge about staff recordkeeping responsibilities;

The survey provides a mechanism for staff to highlight aspects of the training course and to provide feedback about any other area of the University’s recordkeeping program;

The availability of survey data facilitates the University’s compliance with its annual reporting requirements under the State Records Act 2000 to provide an assessment of the efficiency and effectiveness of its recordkeeping training program;

The survey data is useful in conjunction with key performance indicators for validating the training program and justifying to senior management the University’s significant investment in online training.
5. Security, Confidentiality and Privacy

5.1 Security

The University’s records are a vital information asset and must be protected against unauthorised access, disclosure, accidental loss, arbitrary disposal, and corruption. The Records Management & Archives Office approaches security issues within a framework that encompasses a number of different areas.

- **Systems security** - the electronic systems of the Records Management & Archives Office includes its main records management database HP-TRIM, and its support APEX information databases.

As a strategic information management system, ITS apply the highest level of network security and back-up protocols to the TRIM records management system. Daily security backups of data and weekly back-ups to a remote location (the Rockingham Campus) provide for the recovery of data and protection against information corruption and loss. Security protocols monitor access and attempted breaches of security. Access, which is via a username and password, is restricted to authorised staff.

The APEX information databases are accessed via the Murdoch Authentication and Identification System (MAIS), i.e. via a valid Murdoch username and password. The databases are backed up nightly and the backups transferred to the Rockingham Campus on a weekly basis.

In compliance with the University’s *IT Password Procedure*, the Records Management & Archives Office is required to change its passwords every 6 months.

- **Security of premises** – The Records Management & Archives Office consists of room 1.007 located in building 128, and room 1.003 which is the Archives facility located in the Chancellery building. Access to these rooms is restricted to authorised staff. Both rooms are fitted with thermal (i.e. heat) detectors that are linked to the University’s automatic fire detection and alarm system and monitored by the WA Fire Brigade and the University’s Security Office.

- **Migration** – electronic records are subject to a dynamic preservation environment and must be migrated through successive changes in hardware and software to ensure they retain their structure, integrity and useability. Without a systematic process, access to and useability of electronic records can easily be lost, resulting in harm to the University and a breach of its obligations under the *State Records Act 2000*. Refer s.11 Data Migration;

---

3 Refer s.3 Records Management System
● **Metadata**: the Records Management & Archives Office uses metadata for a range of recordkeeping requirements including the exercise of control over access to confidential records and the use of audit trails that show which staff, and when, have accessed a record. *Refer s.13 Metadata Requirements;*

● **Training program**: the Records Management & Archives Office manages an online recordkeeping awareness training program. This aims to raise staff awareness about their recordkeeping responsibilities including the requirement to protect and keep secure the records held in their custody. *Refer s.4.12 Recordkeeping Training Program;*

● **Access to records** – proper access controls are essential in order to safeguard the University against the indiscriminate release and disclosure of information. Access to records incorporates system design as well the observance of legal and procedural requirements. Records staff shall apply appropriate access and security protocols to all confidential and sensitive records. *Refer s.6 Access to Records;*

● **Disaster planning and recovery**: a current disaster preparedness and recovery plan incorporates essential planning for security issues;

● **Legal disposal of records**: the University is required by law and corporate governance requirements to protect its records from unauthorised and premature destruction. The arbitrary disposal of university records represents a serious breach of its legislative and organisational accountability requirements. Staff must dispose of records strictly in accordance with university policy and authorised disposal authorities. *Refer s.15 Retention and Disposal.*

### 5.2 Confidentiality

The University routinely receives, creates and manages confidential information about students, staff, external organisations and government agencies. All employees have a duty to respect the confidential nature of these records.

Information that is available in the public domain is not confidential. Consequently, staff should avoid applying confidentiality caveats to records in a sweeping fashion.

Examples of confidential records managed by the University include:

- Academic planning;
- Commercial-in-confidence documentation;
- Confidential research data;
- Enterprise bargaining negotiations;
- Financial data including payment card information;
- Industrial relations negotiations;
- Legal contracts & agreements;
• Marketing planning, analysis and strategies;
• Official reviews, audits, and investigations;
• Patient files maintained by the Health and Counselling Service;
• Personal information about staff and students;
• Strategic planning.

The release of confidential records must not be held back where the University is legally required to disclose the records under a court order, Freedom of Information request or official audit.

Confidential information must not be used in any way other than for the purpose for which it was provided. Accordingly, the following safeguards are needed to protect and restrict the use of confidential information:

• Confidential records should be kept in secure storage where access can be monitored and limited to authorised staff. This includes use of lockable cabinets for confidential files and loose documents, and computing systems that meet appropriate network security and access control standards;
• Custodians of confidential information have a duty of care to ensure the proper storage, security, access and release of confidential information;
• Staff with authorised access to confidential information must maintain that confidentiality and not disclose or allow to be disclosed to any person any confidential information;
• There must be no unauthorised access, printing, copying and disclosure of confidential information;
• Staff associated with a confidential research project should sign a relevant confidentiality agreement where applicable;
• Confidential records must never be placed in recycling bins when disposal action is undertaken. They must only be disposed by confidential shredding.

The unauthorised disclosure, loss or misuse of confidential information can have severe consequences including:

• Harm to the University’s reputation;
• Harm and embarrassment to the organisations or individuals that provided the information;
• Unfair commercial advantage given to an organisation submitting a tender for a university contract;
• Advantage given to the University’s competitors;
• Integrity of inquiries or official investigations put at risk;
• Breach of confidence where disclosure of cutting-edge scientific research data is unauthorised;
• Possible legal action against the University.

5.3 Privacy

Privacy concerns the collection, storage and security of personal information, and safeguards against loss, unauthorised access, use, misuse, modification, or disclosure of personal information to third parties. Any information that identifies an individual is regarded as personal information.

Privacy and data protection legislation doesn’t currently exist in Western Australia. However, it is expected that WA will eventually follow other states that have already passed privacy legislation (NSW 1998, Victoria 2000).

Murdoch University has developed a privacy policy in line with general privacy principles. The policy applies to staff, students and the general public.

The University only collects personal information when it is necessary for administrative needs or to meet legislative requirements. Personal information collected by the University about its students and employees includes, but is not limited to: names, addresses, dates of birth, employment details, educational qualifications and progress, financial information, and medical information.

The University has strict requirements about how personal information is managed. Through policies, procedures and protocols it seeks to safeguard personal information collected about an individual by ensuring high standards for storage and security, preventing loss of information, unauthorised access, disclosure to third parties, the alteration of information, and how the information is destroyed or deleted from its recordkeeping and computing systems.

The University does not disclose personal information to outside agencies except where the University is required to do so by legislative requirements or court orders where personal information may be required as evidence in court and tribunal proceedings.

Subject to a number of exceptions detailed in the University’s Privacy Policy, the University undertakes to not use or disclose personal information other than for the primary purposes for which it is collected. Examples of these exceptions include the release of data to authorised government agencies, to professional bodies and schools for purposes of enabling students to undertake a practical experience/clinical component of their course, and to universities for advanced standing requirements and where students have cross-institutional enrolments or are enrolled in a study abroad program.

However, the graduate name, conferral date and award title for each student that has graduated from the University is published on the University’s Graduate Register. This information is in the public domain and permits any third party to confirm whether a person is a graduate from the University with a particular qualification.
‘Sensitive information’ is a sub-set of personal information. It is distinguished from non-sensitive personal information by the legal requirement (Australian Privacy Principle 3.3) that it must not be collected unless the individual consents to the collection of the information. Consequently, the University has very stringent controls over the disclosure of sensitive information.

Examples of sensitive information include information about an individual’s racial or ethnic origin, religious beliefs or affiliations, criminal record, and health information. Some of these examples have relevance to indigenous and international student files. For example, information contained in certified copies of visa and passport details may be sufficient to allow an opinion to be ascertained about an individual’s racial origin or ethnicity, and in some cases about their likely religious beliefs.
6. Access to Records

6.1 Access Guidelines

Timely access to information is essential in order for the University to function effectively and efficiently. A fundamental premise is that all records received or created by staff in the course of the performance of their duties are considered to be official university records and these records must be kept available and accessible to authorised staff and external agencies.

The general right to access records is limited by a number of factors including legislation, legal reasons, confidentiality and privacy considerations, commercial reasons, and official university policy.

Staff are authorised to access records according to the specific delegated authority of their position and the relevance of the information to the performance of their duties. In some cases higher authorisation may be required before access is granted.

The indiscriminate disclosure of information can seriously impact the University. Therefore, staff should be aware that restrictions apply where confidentiality and privacy considerations are relevant.

The following guidelines concerning access to records should be observed by all staff:

- The design of recordkeeping systems must incorporate appropriate security considerations that protect records from unauthorised access;
- A staff member’s right to access records is determined by the relevance of the records to their duties, on a need-to-know basis;
- Access to records is restricted where confidentiality and privacy considerations, including legal professional privilege and commercial-in-confidence issues, are relevant;
- Unhindered access to records must be provided to authorised agencies such as the Office of the Auditor General, Freedom of Information Commissioner, Ombudsman, and the Corruption and Crime Commission;
- The University is required to comply with legal processes such as discovery and subpoena that provide a right of access to its records by the legal system;
- Staff must not breach provisions in confidentiality agreements concerning the access and disclosure of information;
- Access is not permitted to archival records where access restrictions have been approved by the State Records Commission;
- Where there exists risk of exposing the University to potential liability, staff should seek the advice of the University’s Legal Services before releasing information to third parties.
The Recordkeeping Policy and Recordkeeping Guideline provide further guidance in relation to the authorised access to records.

6.2 Public Access to Records

The Freedom of Information Act 1992 provides members of the public with a general right of access to information held by public agencies. The general premise of FOI legislation is that information should be made available unless there is a reason given in the legislation to refuse access.

Exemption categories include personal information about individuals, research information, commercially-sensitive information such as trade secrets, confidential communications obtained in confidence, and records that would be privileged from production in legal proceedings on the grounds of legal professional privilege.

Reasons for not making information available include the potential for litigation, administrative costs of providing information, and the right to privacy of third parties. However, it should be noted that failure to disclose all documents may be construed as a deliberate attempt to hide some documents from public scrutiny and hence constitute a breach of the University’s obligations under the Freedom of Information Act.

Staff should note that it is illegal to conceal, destroy or dispose of a document in order to deny access to it, regardless of whether or not an application for access under FOI has been made. Refer s. 2 Legislation.
7. **File Titling, Classifying and Filing**

7.1 **Classification System**

The Records Management & Archives Office uses a subject-based classification scheme to control the titling of central administrative files managed by the Office. The classification scheme is intended to ensure consistency in the titling of files. The use of controlled language for file titling ensures that the filing system is organised in a structured way reflecting established records management conventions.

The classification scheme has a hierarchical structure in which records are aggregated at four levels including a free-text level if required. The structure consists of ten broad function areas that describe the major function areas of the University. All administrative files held in the Records Management & Archives Office fit into one of these ten broad categories. They are:

- 01 - Academic Activities
- 02 - General Administration
- 03 - Finance and Business
- 04 - Legislative
- 05 - Organisation and Structure
- 06 - Physical Activities
- 07 - Services
- 08 - Staffing
- 09 - Student Matters
- 10 - Legal Services

The categories are progressively broken down to a more specific level, to primary subject areas designated by keywords. Each keyword is further narrowed by one or two specific descriptors. As mentioned above, there is flexibility to add free text as a final-level descriptor if required. Each level of classification equates to a unique file number sequence. For example, 01-03-004-001:

- 01 - Academic Activities (CATEGORY)
- 03 - Assessment (KEYWORD)
- 004 - Examinations (1st DESCRIPTOR)
- 001 - Policies and Procedures (2nd DESCRIPTOR)

Acronyms should not be used in place of the full text but may be shown in parentheses after the full title is shown, for example, National Health & Medical Research Council (NHMRC).

The following benefits accrue from the use of controlled vocabulary and consistency in file titling:

- Facilitates ready access to files and the sharing of information;
• Avoids the unnecessary creation of superfluous files - many of which would contain only limited records;
• Ensures high accuracy and quick response times when database searches are performed and it significantly reduces the return of unrelated search results;
• Facilitates the retrieval of related records and information;
• Facilitates the efficient disposal of records that have satisfied retention requirements.

A unique file number also provides a means by which files can be logically arranged in the compactus ensuring they can be efficiently retrieved when needed. Unique file numbers also facilitate the logging in/out of files and the undertaking of files census activities.

7.2 Classifying Correspondence

Classifying is the process that helps describe, organise, control and retrieve records. It involves analysing and determining the content of a document, consulting the Classification Manual for the appropriate subject category and selecting an appropriate file and, where necessary, creating new descriptor levels in the manual for new files.

The classification of files and records requires a methodical and consistent approach. This helps to facilitate the efficient retrieval of information when it is needed at a later date and ensures that all documentation pertaining to a particular subject is placed on the same file or related file/s.

The classifying of correspondence to relevant central files is the responsibility of the Records Manager. The Records Manager is required to:

• Ensure that records managed by the Records Management & Archives Office are organised into appropriate administrative files so that these records are readily available and accessible to authorised officers of the University;
• Classify records according to their subject content and not the originating person or Office;
• Ensure policy and procedural records are classified to separate files and not to files that hold routine and operational documents even when they relate to the same subject;
• Copy correspondence to all relevant files when it relates to more than one file;
• Enter summary information about correspondence that is of an ambiguous nature in the recordkeeping system’s correspondence-tracking module. Summary details required are: the file number of the file to which the correspondence is classified, title and/or brief description of the correspondence, originator and recipient of the correspondence, and date of the correspondence;
• File numbers are written in pencil at the top right hand corner of the document.
7.3 Filing of Correspondence

- The Records Officer is responsible for the accurate filing of all correspondence on central file. This function is performed on a weekly basis to ensure files are kept up-to-date and to prevent the accumulation of backlogs of filing;
- The Records Officer is to make a brief reading of the correspondence before it is placed on file and check it against the file’s title. This serves as a final check that the correct classification for correspondence has been selected as well as a check to ensure the correct file has been removed from the compactus;
- Correspondence is placed on file in strict chronological order;
- Copies of documentation are not placed on file unless they have annotations that elaborate on a matter and therefore require the document to be kept;
- Where an index is maintained for a central file (see s.7.4) each page must be numbered;
- Filing of Committee minutes - refer s.9.4;
- Original signed legal documents are never hole-punched and placed on file but maintained as loose documents in legal business cartons in the Records Management & Archives Office;
- The Records Officer shall prepare a weekly listing of all outstanding filing for reference purposes by the Records Management & Archives Office. The Records Officer is required to bring all outstanding filing up-to-date on a monthly basis. Where necessary, the Records Officer is to visit offices or request the temporary return of files in order to place outstanding filing on central files that are on loan.

7.4 Indexes

- The use of indexes as finding aids are used for a number of central files and provide staff with an efficient means of locating correspondence on files. Indexes are useful for all files but because of time constraints are limited to selected files;
- An index provides a list, in alpha order, of all documentation on a file. It includes the date of the correspondence, a brief summary of the subject matter and the corresponding page number. Indexes are maintained on the inside cover of central files (in a plastic pocket) and are updated each time documentation is added to the file. Indexes are typically maintained as a Microsoft Word document;
- Examples of files where indexes are maintained include Outside Studies Program Reports, General Complaints, academic links with outside bodies, and general consultancies.

7.5 Shelf Collection

A collection of hard copy university and non-university publications are held in the Records Management & Archives ‘Shelf Collection’. These publications are available for loan by all staff. They include publications from government agencies, Murdoch University, and other Australian universities.
8. Central Files

Central administrative files are created by the Records Management & Archives Office as a means of organising the paper records received and managed by the Office and to facilitate records management functions. These files ensure that large volumes of loose documents are properly and consistently organised, secured and protected. It allows these records to be made readily available for loan and enables their efficient disposal at the end of their retention period.

8.1 Arrangement of Files

Central files are arranged laterally and numerically in a sliding compactus according to the ten major categories identified in the Classification Manual (s.7.1). The compactus has a separate section for closed files to distinguish them from current active files.

8.2 Borrowing Central Files

- Central files are available for loan by all authorised staff;
- Files may be requested by phoning the Records Management & Archives Office or via email. Details of the file number should be provided if it is known (all central file numbers can be found on the Central Files Locator - refer s. 3.2.1). If a file number or the file title is not known, then a description of the file or of the correspondence being sought will assist Records staff in locating the appropriate file;
- Staff requesting a file will be advised if it is logged out to another officer. The Records Management Office should be notified if the file is retrieved from the officer to allow the borrower location to be updated;
- Central files are logged out to a staff member’s name and not to their position title. The records management borrowers’ directory is set up this way to allow for staff movements over time and to establish personal accountability;
- Staff should avoid holding on to central files for longer than is necessary, especially when the file requires the attention of several officers;
- Files borrowed from the University Archives or from offsite storage must have the appropriate adhesive label affixed to them. These are ‘Murdoch University Archives’ for files from the Archives and ‘Offsite Storage’ for files from offsite storage;

These files must also have a ‘File Location’ label applied, i.e. the shelf or container number. These measures facilitate the return of files to their correct ‘home’ location and prevent them being mistakenly returned to the compactus in the Records Management Office that is reserved for current active files;
- When staff cease employment with the University they must return all central files to the Records Management & Archives Office. They must advise if any files will be retained for use by their successor.
8.3 How Long Can a File be Loaned?

- There is no definite loan period. However, central files should not be kept for lengthy periods of time. All central files are permanently housed in the Records Management Office and files should be returned when they are no longer being actively used;
- If action on a file is dependent on the procurement of external advice or if time to tend to the file does not currently permit, staff should use the bring-forward system and return the file to the Records Office for return at a later date specified by the officer (refer s.8.8);
- Files that are in use must be kept readily accessible for the convenience of other staff, and to facilitate monthly census activities performed by the Records Officer, and to allow files to be easily updated with correspondence.

8.4 Returning Files to the Records Management Office

- Staff should return files to the Records Management Office as soon as action on a file has been completed;
- Officers should initial and date the front of a file before returning it to the Records Management Office. Files can be returned by placing them in collection trays arranged with the Records Management Office or via internal mail or in person;
- Confidential files must be placed in a sealed envelope before placing in a collection tray or returned in person to the Records Management Office;
- When files are logged back into the system by the Records Officer, files must be checked to determine if another officer needs to see the file or if a bring-forward entry is required. Loose correspondence placed inside the file must be checked and secured to the file. The most recent correspondence on file must be checked for annotations, file notes or post-it notes that indicate if another officer's attention to the correspondence is required or if the file is to be returned to the officer at a later date;
- If no further action is required on a file then its current location in the recordkeeping system should be changed to the ‘Home Location’ and the file returned to its physical home location, this being the compactus in the Records Office or the University Archives or to offsite storage.

8.5 Transferring Files

- When an officer wishes to transfer a file to another officer, they should write on the file cover ‘File’ or enter the specific page number if the folios are numbered, write the current date and the name of the officer to whom the file is being transferred;
- If the file is transferred to another officer via the Records Office the Records Officer will amend the borrower location on the records management system to reflect the changed location before taking the file to the designated officer;
• When a file is passed directly to another officer the Records Management Office must be notified of the file transfer so that the borrower location can be updated. This may be done by means of completing a yellow file transfer card provided with the file or by contacting the Records Office via telephone or email. Responsibility for a file remains with the borrower until the borrower location is changed on the records management system;

• Failure to advise the Records Office of file movements will result in inaccurate file locations being shown on the records management system. This will result in incorrect advice being provided by the Records Office about a file’s location and consequently a delay in file delivery. It may also result in time unnecessarily being spent searching for missing files.

8.6 Taking Central Files off Campus

If an officer intends to take a central file off the University’s premises, for example for reference use in a meeting or for working at home, they must first notify the Records Management Office.

Since central files contain original correspondence, agreements, and confidential documentation staff should exercise discretion when deciding if a file should be taken off campus. When central files are taken off-campus responsibility for the file lies with the borrower for ensuring the file’s security.

Central files must not be passed to individuals or organisations outside the University without the authorisation of the Records Manager or University Secretary.

8.7 Confidential Files

Special care must be taken to protect confidential files against unauthorised access and disclosure by restricting access to authorised staff only. Refer s.6.1 Access to Records.

Files containing personal information, such as staff and student files, are covered by the University’s privacy policy. Refer s. 5.3 Privacy.

8.8 Booking Files (Bring-Forward Entries)

• If staff wish to have a file returned at a later date for follow-up action they should provide the following details on the front of the file: B/F (Bring-Forward), the date the file is required and their name, e.g. ‘B/F 30/6/2018 John Smith’. These details must be entered on the records management system and the file returned on the date requested;

• The Records Officer will check all returned files for any bring-forward action. Details of the request will be entered on the records management system and a tick (in red ink) will be made to the left of the B/F request shown on the file to indicate that action has been taken;
• The Records Officer will make a daily check on the records management system for Bring-Forward requests and dispatch any files during the morning file delivery;

• The Bring-Forward system obviates the need for officers to retain files for extended periods of time and allows files to be kept readily available for other staff that might require the file.

8.9 Requesting a New File to be created

• There is no requirement to complete an official ‘New File’ form. Staff simply need to direct requests for new files to the Records Management Office via email. Enquiries in relation to new files should be directed to the Records Manager;

• A new file will be created when a suitable file for documents does not currently exist. If the records are confidential the file will be stamped ‘Confidential’ and ‘Restricted’ and the file will be assigned a ‘Restricted Access’ security level on the records management system;

• The creation of separate files for different Offices is discouraged to prevent the scattering of files across Offices where each file only contains part of the picture. Staff from different Offices frequently need to refer to records created by another Office, and having a ‘one stop’ reference point not only encourages administrative efficiencies but ensures that staff have complete information about a matter;

• Files are created within 24 hours of a request being received.

8.10 File Creation Procedures

The Records Manager will first check the Classification Manual and records management system to ensure that a suitable file does not already exist. If there is no suitable file, a new file will be created observing the following procedures:

• The Records Manager will consult the Classification Manual to determine the appropriate category, keyword, descriptors and file number series. Details will be entered onto the ‘New File’ form and passed to the Records Officer for action. The Records Manager will cross-reference the new file with existing central files where required;

• The Records Officer will create the new file details on the HP-TRIM records management system using the HP-TRIM File Plan and will note the new file number on the ‘New File’ form. If necessary, a new level and record series in the file plan will be created. The new file must have an access and security level assigned, a current location selected, and a retention period entered;

• The Records Officer will then manually prepare the file by stencilling the file number on the file cover and printing the keyword and file descriptors (that is, the file title) on an adhesive label and affixing this to the front of the file. The file number is also indicated on the side of the file by the application of coloured file number labels;
If the file is cross-referenced with an existing file, both files must have the relevant file number and title entered on the file cover as well as entered on the records management system;

Apply security classifications and access restrictions to files that contain confidential information. Confidential files must be stamped ‘Confidential’ and ‘Restricted’;

A ‘File Handling Procedures’ notice must be attached to the inside cover of the file and an ‘ALWAYS quote this file number as your reference on ALL correspondence’ label attached to the file cover. File transfer cards must be attached to the front of the file where applicable;

Barcode labels that uniquely identify a file for files census purposes and other records management functions must be printed and attached to the front and back of the file cover;

File details must be entered onto the ‘Central Files’ APEX database. Where the file title reveals confidential information the ‘sensitive’ box must be selected to restrict this information to the Records Management Office only;

File details must be added to the Classification Manual MS Word document and manually written in the hard copy manuals used by the Records Manager and Records Officer. This ensures that day-to-day reference listings are always up-to-date;

When the file has been created, the Records Officer will place the ‘New File’ form in the Records Manager’s inwards tray. The Records Manager will check all data entries for new files to ensure the accuracy and reliability of the databases are maintained.

### 8.11 Closure of Files

When a central file is full it should be closed on the records management system and, if required, a new volume created on the system. The records management system will automatically assign the next incremental volume number to the file of the new volume. It will also index all volumes of the same file number together to ensure all volumes are displayed when a search for the file number is performed;

The Records Officer will place a ‘Closed File’ cover sheet as the last folio on the central file. The following information must be entered on each ‘Closed File’ cover sheet: file number, dates covered by documentation on the file (that is, date of the earliest correspondence and date of the latest correspondence), signature of the Records Officer, date of closure, and reference to the next volume if required;

A ‘Closed Volume’ adhesive label must be applied to the file cover to indicate its closed status. The closed file is then transferred to the Closed Files Section of the compactus;

A new hardcopy volume will be created and placed in the current files section of the compactus.
8.12 **Lost Files**

The following steps are required when a central file cannot be located:

- Records staff will make a thorough search of the compactus and the Records Management Office to see if the file has been misfiled;
- The borrower history on the records management system will be checked to determine which staff have previously loaned the file and might therefore be expected to have the file;
- Email messages should be sent to staff with details of the missing file. This will include the file number and file title. Staff are to be requested to check to see if they have the file or if they recall having seen it recently;
- If the file cannot be found, all Offices that may possibly have the file shall be physically searched by Records Management staff;
- A file is assumed to be lost if it cannot be located are taking all necessary steps to find it. A replacement file should be created with the words ‘REPLACEMENT FILE’ clearly displayed on the cover of the file;
- An effort should be made to obtain copies of records that were filed on the lost file by searching related files and requesting copies from staff;
- Undertaking regular files census activities reduces the risk of files being misplaced or lost.

8.13 **Annual Review, Cull and Disposal**

An annual cull of files in the Records Management Office is to be undertaken by the Records Manager & Archivist. The compactus accumulates large volumes of records during the year, and it is necessary to create storage space while also preventing damage to files caused by forcing them into crammed shelving spaces.

As with all records of the University, the records contained on central files must be kept for varying periods of time in accordance with officially approved disposal authorities. The disposition action taken on each central file is determined by the subject matter of the file. There are three outcomes for files culled from the compactus. These are:

- Transfer files with archival value to the Archives facility for permanent retention;
- Transfer files with future destruction dates to offsite storage; and
- Arrange immediate destruction of any files where the retention period has already been met.
9. **Committees**

A sizeable volume of the University’s records are produced by its committees. These committees frequently establish sub-committees and working parties for the purpose of undertaking research, consultation and discussion and then reporting their findings and recommendations to the higher committee. Working parties are established for a limited and specific purpose and are disbanded after their final report has been presented to the relevant committee.

Committees have significant delegated authority to make decisions, take action, decide policy and procedure, undertake academic and strategic planning, authorise expenditure etc. The records created by committees and their working parties characteristically consist of agendas, minutes, reports and associated papers. These records often have permanent retention requirements and it is essential they are managed correctly.

An agenda consisting of ordered items for discussion is produced by a committee’s secretary and distributed several days ahead of a meeting to committee members with copies provided to other interested parties including the Records Management & Archives Office. The deliberations and decisions taken at a meeting are recorded by the committee’s secretary. The resultant ‘minutes’ are subsequently confirmed, subject to any amendments, as a faithful account of the proceedings at the next committee meeting.

9.1 **Recordkeeping Requirements**

Agendas, minutes and reports produced by committees and their working parties must be managed in accordance with the requirements of the *State Records Act 2000* and the University’s Recordkeeping Policy. In particular, the requirements to create proper and adequate records of a committee’s activities and retain them as evidence of good governance for a period of time specified in authorised disposal authorities must be observed.

The Records Management & Archives Office maintains central files for records created by the main University committees and working parties. It is the responsibility of the committee secretary to send copies of agendas, minutes, and reports created by the committees to the Records Office for retention on central file. Confidential items and papers tabled separately at meetings must be included but routine and miscellaneous correspondence is not required.

The records generated by the University’s committees form an important part of its corporate memory. The records of many of these committees have permanent retention requirements and must be retained in accordance with university policy and statutory requirements including SRC Standard 7: *State Archives Retained by Government Organisations* and State Records Office Policy 8: *Policy for the ongoing management of electronic records designated as having archival value*. Relevant committees include the Senate and its standing committees, Academic Council and its standing committees, and the Board of Examiners.
The agendas, minutes and associated papers of minor committees are not required by the Records Management & Archives Office. These records must be retained by the School for 5 years after last action, after which they can be destroyed.

9.2 External Committees

- Where the University has significant input into an external committee or where it has a coordinating or secretariat role, relating to strategic planning and policy, corporate executive, or core business functions the agendas, minutes, reports and supporting papers of the committee must be retained permanently;

- Where the University has a limited or no coordinating role with an external committee the agendas, minutes, reports and supporting papers of the committee must be retained for 5 years after last action, after which they can be destroyed;

- Committee minutes and agendas received from external committees with which the University has no involvement may be destroyed at any time.

9.3 Meetings

- The University frequently conducts recordable activities at meetings. These may include high-level meetings involving senior management, industry delegates, and trade union officials, as well as routine meetings at any Office or School level;

- It is necessary to create a record of the discussions and decisions reached at a meeting particularly where matters of core business are discussed and decisions are made. The record may consist of a formal agenda and minutes or a file note that indicates the date the meeting was held, who was in attendance, and a summary of the key points and outcomes of the meeting;

- As with all records of the University, the records generated by meetings must be retained according to the retention requirements shown in SRC authorised disposal authorities.

9.4 Filing of Agendas and Minutes

- The Records Officer has responsibility for filing agendas, minutes, reports and supporting papers on central file;

- The Records Officer shall periodically check relevant central files to ensure that holdings on files are complete and up-to-date. When placing minutes and agendas on file the Records Officer will also check that minutes and agendas of previous meetings have been received by referring to the ‘confirmation of previous minutes’ sub-heading in the minutes;

- Where the minutes of a committee meeting are missing, the Records Officer will check the agenda to establish if the minutes are attached to the agenda and, if so, will make a copy of the minutes for placement on file. If the minutes are not
provided with the agenda, the Records Officer will contact the committee’s secretary and request a copy of the missing minutes;

- Original minute books of the Senate and Academic Council and their standing committees shall be maintained in the University Archives.

9.5 Extracts of Committee Resolutions

- The Records Manager is to ensure that copies are made of significant discussions and resolutions of Senate and Academic Council and placed on the appropriate central files. Sometimes a resolution applies to two or more files in which case copies will be placed on all relevant files.
10. **Disaster Management**

In accordance with the requirements of the *State Records Act 2000* and the University’s *Recordkeeping Policy* the Records Management & Archives Office has established a *Counter Disaster and Recovery Plan – University Records* for the records in its custody. In particular, this plan covers records in hard copy format. Guidelines for the long-term preservation of electronic records are included at s.11 Data Migration. Disaster recovery planning for electronic records and for protecting computer systems and infrastructure is managed by the Audit and Risk Management Office.

10.1 **What is a Disaster?**

A disaster is typically an unexpected event that creates a potential inability on the University’s part to provide critical business functions for a period of time and which has potential long-term adverse effects on its normal operations.

The causes of disasters are varied. They can be building-related such as a fire caused by faulty wiring, or flooding caused by a burst pipe. They can have their origins in information technology including, for example, deliberate or accidental erasure of electronic data, computer viruses causing corruption of data, and computer equipment failure leading to loss of data. Natural events such as seismic disturbance, flooding, bushfires, lightning strikes and cyclones, or criminal behaviour and industrial accidents can also be the cause. Some disasters can unfold gradually such as the (initially) undetected damage to paper records caused by infestations of insects or vermin.

A disaster event that causes significant loss of the University’s records has the potential to cause major disruption to its ability to operate effectively and can lead to significant financial loss, public embarrassment and a loss of credibility and goodwill among its stakeholders. Effective planning is therefore essential for minimising the likelihood of a disaster event occurring and mitigating the impact and costs of salvage and restoration activities following the occurrence of an actual disaster event.

10.2 **Counter Disaster and Recovery Plan**

The University’s *Counter Disaster and Recovery Plan – University Records* is a document that sets out strategies for preventing disasters that may impact on the University’s records, and for preparing an appropriate response to and recovery from disasters should they occur. The Plan covers risk assessment, analysis, planning, counter disaster measures, vital records, disaster response, and recovery of records.

10.3 **Vital Records**

The disaster plan addresses the identification and protection of ‘vital records’. These records are considered vital because they contain information essential to the execution of the University’s fundamental responsibilities, and without which the University could not continue to operate. Vital records are considered to be irreplaceable and mission-critical records, hence the need to specially protect them. Their format is immaterial and
may consist of hardcopy, electronic or other media. They typically constitute 3%-10% of an organisation's records.

Vital records establish and protect the legal and financial rights and interests of the University, and of its employees, students and clients. They must be prioritised for recovery and restoration operations in the event of a disaster to allow the University to continue to comply with its legislative obligations.

The most common method used by the Records Management & Archives Office for protecting hardcopy vital records is to make copies of the originals for regular operational needs and keep the copies in a location separate from where the originals are stored. This ensures the originals are protected from unauthorised access, accidental loss or destruction. The use of specialised storage equipment provides a very high level of protective custody from theft, fire and water damage. A fireproof filing cabinet housed in the Archives facility offers excellent protection from fire and features a high-security locking mechanism.

10.4 Responsibility for the Disaster Plan

The Manager Records Management & Archives has responsibility for reviewing and updating the Counter Disaster and Recovery Plan - University Records and for implementing the strategies explained in the Plan.
11. Data Migration

11.1 Introduction

Digital records must be preserved and maintained over time for as long as required to meet various administrative, legal, fiscal and archival requirements.

Digital records face the challenge of a dynamic preservation environment. Inherent technological obsolescence means that operating systems and software applications have limited lives and will be inevitably upgraded as faster systems with improved functionalities become available. Many records, however, have retention periods greater than one generation of technology.

Digital records must therefore be periodically transferred (migrated) from their current environment to a new one to ensure they remain usable and properly maintained for the duration of their retention requirements. Since digital records are fragile and easily corrupted or altered the migration of digital records through successive upgrades of hardware and software must be undertaken in a carefully managed and documented process.

The migration process must ensure that digital records remain accessible and usable and without any loss of integrity or authenticity of the records. Associated metadata that describes the content, structure and context of the records must also be preserved during the migration process.

Furthermore, the University must be able to show that its procedures for maintaining digital records through time ensure the trustworthiness and reliability of the records and that they can be relied upon, if needed, as admissible evidence in a court of law.

A failure to manage digital records in accordance with management and other stakeholder expectations can constitute a failure in organisational accountability and a breach of legislative requirements.

The facilitation of legislation such as the Electronic Transactions Act 2003, the Freedom of Information Act 1992 and, in particular, the State Records Act 2000 can be seriously impeded if the University fails in its responsibilities to ensure the ongoing availability of its digital records.

State Records Commission (SRC) Standard 8 “Managing Digital Information” provides a number of minimum compliance requirements that organisations must observe to ensure the long-term preservation of digital records and their ongoing accessibility and usability. These are incorporated at sections 12.6-12.8.

4 Refer s. 11.3 Requirements of the State Records Act 2000
11.2 Definition of Terms

Authentic record - an authentic record is one that can be proven to be what it purports to be (i.e. the content is what it appears to be, it was created by the person who appears to have created it and it was created at the time it appears to have been created);

Conversion - the process of changing records from one medium to another, or from one format to another;

Digital record - any digitally produced or stored record of information within the meaning of Section 3 of the State Records Act 2000 that exists in binary form and that requires combinations of computer hardware and software to be read and understood;

Integrity - the integrity of a record refers to its being complete and with no unauthorised alterations. Note that records can be altered and retain their integrity provided the alterations are allowed by policy, are authorised, and are documented;

Integrity check - a mechanism to verify that the present state of data does not involve tampering, modification or bit loss in a manner that compromises authenticity, completeness and reliability;

Long-term - greater than one generation of technology;

Migration - the process of transferring electronic records from one computer system to another, while maintaining the records' authenticity, integrity, reliability, and useability;

Preservation - the process and operations involved in ensuring the technical and intellectual survival of authentic records through time;

Recordkeeping metadata - data describing the context, content and structure of records and their management over time.

11.3 Requirements of the State Records Act 2000

- Digital records must be protected and preserved for the duration of their retention requirements to ensure their ongoing accessibility and usability;
- Digital storage media should be monitored and periodically refreshed to prevent data loss through media degradation and obsolescence;
- Planning, design and implementation of computer systems must include provision for conversion or migration of digitised records for the entire life of the record.


11.4 Scope

All electronic information and records held in all recordkeeping and corporate business systems, network drives and electronic storage devices at Murdoch University are covered by these guidelines.
11.5 Essential Characteristics of Records that must be Maintained through the Migration Process

For the duration of their retention requirements, digital records must retain the following essential characteristics while being managed and maintained in electronic recordkeeping systems:

- **Authenticity** – a record can be proven to be what it purports to be, to have been created or sent by the person that created or sent it, and to have been created or sent at the time it is purported to have occurred;
- **Reliability** – a reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities;
- **Integrity** – a record must be complete and unaltered, and protected against unauthorised alteration. This characteristic is also referred to as ‘inviolability’;
- **Usability** – a record can be located, retrieved, presented and interpreted.

11.6 Principles

The following principles must guide the planning, processes and outcomes of any data migration exercise undertaken by the University:

- Digital records will be migrated through changes in the hardware and software environment and the records will retain their structure, content and context for the required duration of their retention periods;
- All links between digital records and their associated metadata will be retained when records are migrated and will be maintained and kept usable for the life of the records;
- The migration process will ensure that the authenticity, reliability, integrity and usability of digital records are maintained and that the records remain accessible;
- Digital records in legacy systems will be maintained until migrated records in the new system have been fully validated and the system become operational;
- The authenticity and integrity of migrated records will be checked and verified by comparing data between the old and new databases;
- Migration of digital records, including records of permanent (archival) value, will be in accordance with SRC Standard 8: Managing Digital Information.

11.7 Responsibilities

Information systems administrators are responsible for:

- Implementing appropriate migration strategies to ensure the continued availability of the digital records for as long as they are required to be kept;
● Ensuring that the essential characteristics of digital records are not changed by the migration process (refer s. 11.5);
● Periodically monitoring digital storage equipment and software and determining if migration of data is required.

11.8 Data Migration Procedures

The migration of digital records and their associated metadata must be a well-managed and documented process. It is essential the records are migrated using strictly controlled procedures and that all authorised changes are rigorously documented.

The following systematic procedures should be followed when digital records need to be migrated in order to ensure they remain available and useable by staff for as long as required:

● Determine which records need to be migrated, and document summary details;
● Refer to authorised disposal authorities to determine if any of the records can be destroyed prior to migration;
● Determine if the retention periods of records identified for migration should be re-appraised;
● Ensure appropriate migration programs/scripts are selected for the migration process and signed-off by an appropriate IT manager;
● Risks associated with the migration process should be assessed and documented;
● Undertake trial migration to test the migration process and evaluate and document the outcomes;
● Conduct the migration of records and their associated metadata, and document the process;
● Verify the completeness and integrity of the migrated records and their metadata to ensure their continued readability, authenticity and reliability. The results, including any alterations to the records as a result of the migration exercise, and any inaccuracies and “unrecoverable” errors that were identified should be documented;
● Review the migration process and the methodology that was used.

11.9 Compression

Computer files are sometimes stored in compressed formats. The function of compression is to maximise available storage space and minimise the bandwidth requirements when files are transmitted over computer networks.

The main concerns that records management has about the use of compression techniques are:
● Compressed files can pose problems for the retention of digital records with long-term retention requirements. This is because compression techniques are software dependent and future retrieval of compressed information requires access to appropriate decompression programs;

● The use of compression techniques must be considered within the framework of records management conventions such as authenticity and admissibility. Only “lossless” compression should be used since “lossy” compression techniques discard some aspects of data and this can raise serious questions about the authenticity of the records and their admissibility in a court of law.
12. **Outsourcing Arrangements**

Standard 6 *Outsourcing* issued by the State Records Commission requires all new and renewed contracts or arrangements entered into by the University with external service providers, for purposes of performing a function or activity for or on behalf of the University, to be compliant with the requirements of the *State Records Act 2000*.

Standard 6 makes the University accountable for ensuring that any contractors or consultants it engages clearly understand the University’s accountability requirements under the State Records Act. The Standard has seven Principles covering planning, ownership, control, disposal, access, custody, and contract completion.

Records often remain in the custody of the external party until completion of the contract. Consequently, these contracts must establish the legal ownership of the records including any intellectual property considerations that might arise.

Contractual recordkeeping provisions must also address access requirements (for administrative or litigation purposes) and ensure that obligations are placed on the outside party concerning the proper care of the records until they are returned to the University once the contract is completed.

Further, the Standard requires responsibilities to be addressed relating to correct procedures for the disposal of records created in relation to the functions performed or services provided to the University by service providers. This means that any disposal action can only be undertaken within the framework of authorised retention and disposal authorities.

The University’s Legal Services team has issued a standard clause for use in relevant contracts and service agreements. The clause is adapted as required. Provisions cover areas including the following:

- External parties must comply with the *State Records Act 2000* and any principles or standards developed by the University in accordance with the Act;
- All records created in relation to the functions performed or services provided are to remain the property of Murdoch University;
- The disposal of any records will be in accordance with the University’s Recordkeeping Plan; that is, in accord with its authorised disposal authorities;
- The University is to have unlimited access, on reasonable notice, to all records created by the service provider on behalf of the University;
- On expiry or early termination of any agreement, the external party will either return all such records to the University or destroy them in accordance with the University’s directions.
Examples of functions and services outsourced by the University include the employee assistance program, grounds maintenance, international student recruitment services, office cleaning and waste removal services, pest control services, student accommodation services, and window cleaning services.
13. Metadata Requirements

13.1 Introduction

Recordkeeping metadata may be defined as data describing the context, content and structure of records and their management over time. It consists of descriptive information that is intended to facilitate records management processes and support organisational accountability. Metadata gives context to the content of a record and enables the record to be managed according to recordkeeping principles.

There are various administrative and legislative requirements to create and maintain recordkeeping metadata. SRC Standard 8 ‘Managing Digital Information’, for example, requires organisations to ensure that digital information is captured as evidence of business activity along with associated metadata that describes its content, structure and context.

The records management system incorporates a number of mandatory and optional metadata elements, many of which are automatically generated by the system. The University’s classification system is incorporated in the design of the records management system and this promotes consistency when applying file naming and numbering metadata conventions.

The application of recordkeeping metadata considerably facilitates the accessibility and management of information. It enables records to be found whenever they are needed by providing different search methods for the efficient searching of records, and it allows tight control to be exercised over access to confidential and sensitive information.

The use of metadata to control access to information is extremely important since a large proportion of the University’s records are confidential or attract privacy considerations. These include personal records relating to the University’s staff and its students, records that are commercial-in-confidence, official reviews and investigations, research-based records such as research projects and intellectual property, and legal records that are subject to client-lawyer privilege.

The audit trail provided by metadata elements can be crucial in giving assurances about a record’s authenticity by authoritatively demonstrating who created the record, when it was accessed, modified, and destroyed. The use of metadata also plays an important role in helping to ensure that records are retained for their appropriate retention period before any disposal action can be undertaken.

Managing digital records over time is a dynamic process and metadata can be used to facilitate migration actions. For example, metadata can be used to flag which records have ongoing migration requirements and used to document preservation actions performed on the records. Migrating digital records along with associated metadata is essential to ensuring they continue to be authentic, reliable and useable over time.
The systematic and consistent application of recordkeeping metadata will help to facilitate recordkeeping processes and ensure the University’s records can be relied upon to support the University’s business activities and to meet accountability and legislative requirements.

The metadata requirements outlined in this section underpin the University’s Recordkeeping Policy, in particular the requirements concerning the keeping of proper and accurate records, accessibility issues, retention and disposal of records, and the continued integrity and useability of electronic records through time.

13.2 Benefits of Creating Recordkeeping Metadata

It is essential that records that have been captured into the University’s recordkeeping system can be efficiently retrieved whenever needed. Furthermore, records require sufficient contextual and descriptive metadata to ensure they are meaningful and can be properly managed over time. Accordingly, the creation of recordkeeping metadata serves the following purposes:

- enables the efficient searching for records by utilising various search criteria including search by title, keyword, date, and location;
- enables access to confidential records to be effectively controlled by assigning relevant access/security levels at the time of creation and/or registration into the recordkeeping system;
- ensures records are retained for their minimum retention period, facilitates their efficient and timely disposal, and provides evidence of disposal actions;
- supports organisational accountability, auditing processes and transparency of processes;
- facilitates the migration of digital records through successive upgrades of hardware and software and provides evidence of these activities;
- provides audit trails that show evidence of who has accessed a record and when;
- enables records required under FOI or official investigations to be readily identified and protected; and
- facilitates compliance with legislative and regulatory requirements, and best practice recordkeeping standards.

These benefits readily demonstrate why creating recordkeeping metadata must be seen as an integral component of records management. Adequate contextual information must be created in order to facilitate the University’s business processes and the management of its records through time.

13.3 Responsibilities

The University’s staff have a legal responsibility to ensure that records are properly created and managed. This includes the responsibility to ensure that appropriate metadata is included with the records they create and receive.
The consistent and systematic application of recordkeeping metadata to the records created and received by the Records Management & Archives Office will assist the Office in the effective and responsible management of the records in its custody.

Furthermore, it will maximise the Office’s ability to provide a high standard of client service to users of the Office and to meet the expectations of its statutory environment and other stakeholders.

Records Management & Archives staff are required to observe the following responsibilities pertaining to the creation and maintenance of recordkeeping metadata:

- ensure that mandatory recordkeeping metadata is systematically and consistently applied to all records created and registered in the recordkeeping system and associated databases, and the Microsoft suite of applications;
- ensure that mandatory recordkeeping metadata is systematically and consistently applied to all hardcopy records including correspondence control and file delivery;
- maintain recordkeeping metadata for as long as required by legislative, administrative and technical preservation requirements; and
- ensure the integrity and authenticity of records by ensuring that the recordkeeping system guarantees against any unauthorised modification of a record’s metadata.

### 13.4 Metadata Fields Required in TRIM

The following table is a listing of the recordkeeping metadata elements required for all records created or registered in the TRIM recordkeeping system. Most of these elements are considered mandatory in order to meet legislative requirements under the *State Records Act 2000* but also because their use facilitates the implementation of best practice recordkeeping processes.

The inclusion of these metadata fields will help to ensure the responsible use and management of the University’s records through time.

<table>
<thead>
<tr>
<th>Title</th>
<th>Purpose</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Record Number       | To allocate a numeric code to uniquely identify any record created or registered in TRIM. Search and retrieval of a record by its unique record number must enable only that particular record and no other to be returned. | Mandatory  
The record number assigned for new central files must be in accord with the keyword classification thesaurus (file plan).  
For creation of new records requiring free text titling the record number is system-generated. A new entry cannot be completed without a unique numeric code being assigned. This includes entries for |
| Title | The text used to name the subject of each record. Facilitates searching and retrieval of records by searching on a record’s official title or words contained in the title. | Mandatory
For new central files titling must be controlled by adhering to the keyword classification thesaurus.
All other entries must have a title that accurately represents the record’s content in order to facilitate efficient identification of the record.
Acronyms may only be included in conjunction with the full text of a title. |
| Creator | This element uniquely identifies the officer responsible for creating the record. | Mandatory
The default element value, automatically generated by the system, is the ID of the staff officer logged into TRIM. |
| Date Created | The date the record was created. This information facilitates access to records on the basis of their date of creation. A search may be limited to a specific date or inclusive of a range of dates. | Mandatory
New records created directly in TRIM have a create date automatically generated by the system.
Records not created directly in TRIM will have a create date automatically assigned when they are registered in TRIM. However, the date when the record itself was created must also be captured in TRIM. This date may be shown in “Notes”. |
| Date Registered | The date and time a record is captured into the recordkeeping system. This element contributes to the authenticity and integrity of records. | Mandatory
Automatically generated by the system at the time a record is created or registered in TRIM. |
| **Date Closed** | The date the record was closed. | Mandatory  
Automatically generated by the system when a file is closed and a new volume created. |
|----------------|---------------------------------|--------------------------------------------------|
| **Notes** | Allows for additional descriptive information to be provided about the record, including relevant keywords, than is provided in the title alone. | Optional – recommended  
Use of additional descriptive information should be used where the record title does not provide sufficient information to permit effective searching. |
| **Retention and Disposal** | This element refers to the retention period assigned to a record indicating how long it must be retained before disposal action can be undertaken.  
It acts as a trigger for the authorised disposal of records.  
It provides evidence of accountability and transparency of disposal activities. | Mandatory  
The disposal date must be determined in accord with authorised disposal authorities. |
| **Access Privileges Security** | The purpose is to protect records against any unauthorised use and disclosure. | Mandatory  
The default is “Restricted Access” for records where confidentiality, privacy and access considerations are relevant. |
| **Record Requests** | Permits staff to make a request for delivery of a file on a specified future date.  
For example, a particular matter may need to be actioned or reviewed by a certain date or a periodic report provided for an outside agency. | Optional  
Details of bring-forward requests are entered onto TRIM and checked daily.  
Prevents files from unnecessarily cluttering desk or drawer space.  
Delivery of file acts as a trigger for action. |
| **Home Location** | The usual or “home” location where a record is | Mandatory |

**Records Management & Archives – Procedures Manual**  
67
<table>
<thead>
<tr>
<th><strong>Current Location (Assignee)</strong></th>
<th>The current physical location of the record. Enables accurate tracking and retrieval of files. Reports can be produced of all records currently on loan to any authorised user.</th>
<th>Mandatory</th>
<th>The system default current location is same as home location. Loan of files are logged out to officer name (not position title).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Container</strong></td>
<td>To identify the specific carton and shelf location of records transferred to offsite storage or to the University Archives.</td>
<td>Mandatory</td>
<td>Records transferred to offsite storage or to the University Archives must be assigned a specific carton reference number to facilitate future access.</td>
</tr>
<tr>
<td><strong>Movement History</strong></td>
<td>This element acts as an audit trail by showing when a file has been accessed and by whom.</td>
<td>Mandatory</td>
<td>Automatically generated by the system each time a file is logged out to a member of staff or outside agencies such as State Auditors and legal firms.</td>
</tr>
<tr>
<td><strong>Record Type</strong></td>
<td>To categorise the type of records created or registered in TRIM. Required in order to properly describe different record types to facilitate the control and management of records.</td>
<td>Mandatory</td>
<td>Record types include: archive carton, archival information, central file, correspondence, offsite storage carton, original contracts, shelf collection, Vice-Chancellor’s correspondence. Each record type has unique default</td>
</tr>
<tr>
<td>Related Records</td>
<td>values and file titling conventions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identifies relationships that exist between files, including previous volumes and related files.</td>
<td>Mandatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linking related files facilitates the use and understanding of records by providing the full picture.</td>
<td>Contextual relationship between current and all previous volumes is automatically created by the system whenever a new file volume is created in TRIM.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File numbers and descriptions of related files must be manually entered in “Notes” field.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 13.5 Metadata Required for Microsoft Office Word Documents

A considerable percentage of records are created using the Microsoft Office suite of applications, in particular Word, Outlook and Excel. It is therefore essential that minimum metadata is created for records created using these applications.

When documents are created in MS Word, some metadata is automatically created (however, this information isn’t available with the printed document). The metadata, which is shown under ‘Properties’, includes: location of the document, date document created, date modified, date last accessed, date last printed, number of times document revised, and a number of other options that can be custom-included.

Metadata that must be entered manually includes the title and subject of the document and the name of the person who created the document. Optional metadata may be included under ‘keywords’ and ‘comments’.

### 13.6 Metadata Required for Electronic Mail Transmissions

Electronic mail transmissions are official university records within the meaning of the State Records Act 2000 and therefore are subject to the same recordkeeping requirements as hardcopy records and any other record created by digital media.

As with any record email messages, together with any attachments, must be included in a suitable recordkeeping system and retained as long as required to meet applicable legal, fiscal, administrative or archival retention requirements. Without recordkeeping metadata, email messages cannot be accepted as authentic and reliable evidence of the business activity it purports to be.

It is essential that associated metadata is captured and stored with each email record. Without this metadata the meaning and value of the email as an authentic record is considerably devalued. By way of example, if an email transmission is to be accepted as admissible evidence in a court of law it is necessary to first prove its integrity and authenticity. In other words, and as a minimum, it must be possible to prove that an
email message was sent through a certain server(s), the date and time it was delivered to the recipient, and the date and time it was read by the recipient.

Automatically-generated metadata such as the sender, recipient, date and time is tagged to email transmissions. To facilitate the correct classification of the email record staff should always include a title in the subject heading.

The principal recordkeeping metadata associated with email transmissions (based on the Microsoft Office email client ‘Outlook’) are as follows:

<table>
<thead>
<tr>
<th>Element</th>
<th>Explanation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>The subject/title of the email message</td>
<td>Optional - strongly recommended</td>
</tr>
<tr>
<td>Date sent</td>
<td>Date and time message sent</td>
<td>Mandatory - auto-generated</td>
</tr>
<tr>
<td>Date received</td>
<td>Shows the time when a message was received by the intended recipient</td>
<td>Mandatory - auto-generated</td>
</tr>
<tr>
<td>From</td>
<td>Sender’s identity</td>
<td>Mandatory - auto-generated</td>
</tr>
<tr>
<td>To</td>
<td>The recipient(s) of the email transmission</td>
<td>Mandatory - entered manually</td>
</tr>
<tr>
<td>Cc</td>
<td>Recipients other than the primary recipient of the email message</td>
<td>Optional</td>
</tr>
<tr>
<td>Bcc</td>
<td>Recipients of the email message but whose names are not visible to other recipients of the email</td>
<td>Optional - blind copy recipients are only displayed in the sender’s email copy.</td>
</tr>
<tr>
<td>Message options</td>
<td>These permit the sender to attach importance and sensitivity levels to messages.</td>
<td>Optional - when these options are selected the importance and sensitivity level will be displayed in both electronic and hardcopy (printed) versions of the email.</td>
</tr>
</tbody>
</table>
Security settings | The contents and attachments of confidential messages can be encrypted (scrambled) by using the security settings. The option of adding a digital signature to an email is also available. | Optional
Printed emails do not display these settings when used.

Message ID | A unique identification code assigned by the email client to each message. This may be important when authenticating email. | Optional - but always automatically included.
Displayed under “Properties”.
Not required for filing purposes (hardcopy)

13.7 Metadata Required for Oracle Application Express (Apex) Databases

The Records Management & Archives Office has developed and maintains a number of web-based searchable information databases built on the Oracle Application Express development environment. These Oracle Apex databases include the Senate Minutes, Academic Council Minutes, Resources Committee Minutes, Central Files Locator and Murdoch University Publications Databases. The databases are accessible via the Murdoch Authentication and Identification System (MAIS), i.e. via a valid Murdoch username and password.

The records contained in these databases have already been captured elsewhere in the University’s recordkeeping systems, but they are made available in specialised databases to enable a more efficient dissemination and greater accessibility to the records. It is essential that the completeness and accuracy, including correct formatting, of records maintained in these databases are carefully checked before being published to the intranet to ensure staff confidence in the integrity of the information is maintained.

13.7.1 Senate, Academic Council, Resources Committee Minutes

An entry is required for each item in the relevant committee. The metadata will facilitate reliable and efficient searching and retrieval of records, and ensure the records are displayed in an organised and structured format. The relevant metadata elements required with each entry are shown in the table below. All fields are mandatory.

<table>
<thead>
<tr>
<th>Element</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary heading</td>
<td>The main heading of an agenda item discussed at the committee meeting and as recorded in the minutes. Sub-headings are frequently required for entries.</td>
</tr>
</tbody>
</table>
13.7.2 Murdoch University Publications Database

This database provides summary details of articles appearing in official Murdoch University publications such as ‘On Campus’, ‘Synergy’, ‘In Touch’ and ‘Murdoch News’. The database is selective in that only articles considered to have ongoing administrative or historic value to the University are included. The database covers the years 1975-current.

The purpose of the database is to make summary information contained in the University’s publications readily and efficiently available to staff. The following mandatory metadata elements are required for each entry.

<table>
<thead>
<tr>
<th>Element</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headline</td>
<td>The headline of an article as it appears in the publication</td>
</tr>
<tr>
<td>Synopsis</td>
<td>A brief summary of an article. The summary is very helpful in facilitating resource discovery.</td>
</tr>
<tr>
<td>Keywords</td>
<td>Keywords that summarise the subject matter of an article. The use of keywords facilitates the searching and retrieval of articles covering any particular subject</td>
</tr>
<tr>
<td>Names</td>
<td>The names of people mentioned in an article.</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Publication</td>
<td>The name of the publication in which an article appeared</td>
</tr>
<tr>
<td>Issue date</td>
<td>The issue date of the publication</td>
</tr>
<tr>
<td>Issue year</td>
<td>The year the publication was published</td>
</tr>
<tr>
<td>Volume</td>
<td>The volume number of the publication in which the article appeared</td>
</tr>
<tr>
<td>Issue number</td>
<td>The issue number of the publication in which the article appeared</td>
</tr>
<tr>
<td>Page number</td>
<td>The page number of the publication in which the article appeared</td>
</tr>
</tbody>
</table>

### 13.7.3 Central Files Locator

This database mirrors the central files created and maintained in the TRIM records management system. Its structure reflects the classification scheme used when creating new files. Its purpose is to provide staff with an efficient search tool for identifying central files by entering any number of keywords.

The Central Files Locator includes all files with the exception of files where the file description contains confidential information. This includes, for example, Freedom of Information requests, complaints made to the Parliamentary Commissioner for Administrative Investigations (State Ombudsman) and the Human Rights & Equal Opportunity Commission, and confidential research projects.

The following recordkeeping metadata fields are required for each entry in the Central Files Locator:

<table>
<thead>
<tr>
<th>Element</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Number</td>
<td>The unique record number determined according to the classification thesaurus</td>
</tr>
<tr>
<td>Category</td>
<td>Refers to one of the ten primary categories under which all central files are classified</td>
</tr>
<tr>
<td>Keywords</td>
<td>Reflects the hierarchical structure of the keyword classification system</td>
</tr>
<tr>
<td>First Descriptor</td>
<td>Reflects the hierarchical structure of the keyword classification system</td>
</tr>
</tbody>
</table>
### Second Descriptor
Reflects the hierarchical structure of the keyword classification system

### Third Descriptor
Reflects the hierarchical structure of the keyword classification system

### Fourth Descriptor
This element used if required to provide additional information about a central file including reference details about related files

### Sensitivity
This element must be selected where descriptive information about a file contains personal or confidential information. Selection of this element ensures the file’s details will not be displayed on the University intranet.

#### 13.8 Cartons Stored Offsite - Excel Spreadsheet

This spreadsheet enables the effective control of records transferred to offsite storage. The spreadsheet includes additional information not recorded in TRIM such as the cost centre allocation, the barcode number for each carton, and other relevant information.

The following recordkeeping metadata fields are mandatory for each entry in the Records Stored Offsite spreadsheet:

<table>
<thead>
<tr>
<th>Element</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carton Number</td>
<td>The unique number assigned to a carton that contains records designated for offsite storage.</td>
</tr>
<tr>
<td>Cost Allocation</td>
<td>The provenance of the records. Indicates the Office or School from where the records originated and to which the allocation of relevant offsite storage costs will be assigned.</td>
</tr>
<tr>
<td>Cost Code</td>
<td>The abbreviated cost allocation code required when requesting retrieval of cartons from offsite storage.</td>
</tr>
<tr>
<td>Destroy Year</td>
<td>The date when records in a specific carton are to be destroyed in accord with the retention period indicated by an authorised disposal authority.</td>
</tr>
<tr>
<td>Destroyed</td>
<td>This element is checked “Yes” when written authorization is provided to the offsite storage provider instructing the destruction of cartons listed in the periodic disposal report.</td>
</tr>
<tr>
<td>Element</td>
<td>Explanation</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Date sent offsite</td>
<td>The date when a carton is collected and taken to the offsite storage facility.</td>
</tr>
<tr>
<td>Recall barcode number</td>
<td>The unique 9-digit barcode number provided by the offsite storage provider and that is applied to each carton to facilitate processes.</td>
</tr>
</tbody>
</table>

13.9 Metadata Required for Hardcopy Central Files

The titling of central files must follow standard file naming conventions. The Records Management & Archives Office uses a hierarchical keyword classification scheme that ensures file creation, storage, searching, retrieval and disposal activities are managed in a consistent and organised way.

The following recordkeeping metadata must be applied to all new central files, including new volumes, as a means of controlling and managing the records they hold.

<table>
<thead>
<tr>
<th>Element</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Number</td>
<td>The file number as created in TRIM must be stencilled on the file cover and coloured numeric labels applied to the side of the file to facilitate filing, retrieval and visibility.</td>
</tr>
<tr>
<td>File Title</td>
<td>The file title must be printed on an appropriate adhesive label and attached to the file. The title must include first, second, third and fourth level descriptors in order to provide sufficient descriptive information about the file.</td>
</tr>
<tr>
<td>Barcode Label</td>
<td>The unique barcode number that is automatically assigned in TRIM whenever a new file is created. The barcode number must be printed on an adhesive label and affixed to the file. The purpose of using barcode technology is to provide an efficient means by which to undertake periodic files census activities.</td>
</tr>
<tr>
<td>Borrower</td>
<td>The name of the officer requesting a central file must be written on the file’s cover. Together with the officer’s sign-off (see below) this metadata ensures that an accountable audit trail is created.</td>
</tr>
<tr>
<td>Date borrowed</td>
<td>The date a file is borrowed and logged out to an officer.</td>
</tr>
<tr>
<td>File Sign-off</td>
<td>When staff no longer need a file they must initial and date the file to indicate that action is completed.</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location</td>
<td>The default home storage location for central files is the Records Management &amp; Archives office.</td>
</tr>
<tr>
<td></td>
<td>When a file is retrieved from offsite storage or the University Archives the home storage location must be indicated on the file to ensure correct filing when it is returned to the Records Office.</td>
</tr>
<tr>
<td>Related Files</td>
<td>The file number and title of related files must be cross-referenced on the file cover.</td>
</tr>
<tr>
<td>File access</td>
<td>A file that contains confidential or personal records must be stamped “Confidential” and “Restricted” to ensure that access is properly controlled, and to alert authorised users to any access restrictions that apply to the file.</td>
</tr>
</tbody>
</table>

### 13.10 Retention of Recordkeeping Metadata

Recordkeeping metadata is essentially a record in itself which means it is subject to the requirements of the *State Records Act 2000* and therefore to the same appraisal decisions as other records. As a rule of thumb, most recordkeeping metadata associated with a record must be retained for at least as long as the retention period of the record to which it relates. Frequently it must be retained for a longer retention period.

Retaining recordkeeping metadata elements past the life of a record is an integral aspect of demonstrating organisational accountability. It provides, for example, auditable evidence of the University’s disposal activities and documents the authority for disposal actions. As a minimum, the following recordkeeping metadata elements should be retained past the life of a record: the record number, record title, date created, disposal action, and a record’s log of event history.

The retention of recordkeeping metadata facilitates compliance with legislative requirements concerning the management of electronic records, in particular SRC Standard 8 ‘Managing Digital Information’. The retention of applicable metadata provides evidence about how electronic records have been used and managed over time by providing an audit trail of all actions undertaken on the records and their associated metadata. This includes, for example, metadata relating to migration procedures and integrity checks of migrated records that are undertaken to ensure their continued readability and reliability.

‘Records Disposal Authorisation’ forms must be retained to support organisational accountability and transparency. These forms demonstrate that the University’s records
have been disposed of in accordance with authorised disposal authorities and government regulations. They provide summary information about records for disposal, the dates covered by the records, the format of the records, and reference to the disposal authority applied to the records.
14. Digitisation

14.1 Introduction

Digitisation is the process of converting hard copy records into a digital format. Printed text is the most commonly digitised source material but photographic images, audio and video may also be digitised.

Digitising records can provide significant benefits to the University especially in terms of improving the accessibility of information and enhancing security protocols. Digitisation also facilitates the integration of business information systems when used for improving the efficiency of business processes and the implementation of electronic workflow processes. Further, digitisation projects are an effective disaster preparedness strategy and a useful means for disseminating information to a wider user base.

Digitisation projects can be expensive undertakings and should be properly costed and the benefits realistically explained. Digitisation projects must also comply with legislative requirements established under the provisions of the State Records Act 2000. These include SRC Standard 8 Managing Digital Information – Principle 5 Digitisation and the SRO-issued General Disposal Authority for Source Records and Digitisation Specification.

Murdoch University digitisation projects are required to observe the following procedures. These requirements apply to records in all formats including text documents, photographs, maps and plans, audio recordings, and video and film recordings.

14.2 Project Evaluation

When a digitisation project is proposed, the costs should be carefully weighed against the expected benefits of the project. There are a number of factors that will influence the cost of a digitisation project including the format of the source document, specific conversion specifications, staff time managing the project, and quality checking requirements.

Since most records have limited retention requirements, staff should consult the authorised retention and disposal authorities to determine how long the records need to be kept and whether it is in fact worthwhile undertaking a potentially time-intensive and costly project for records whose retention requirements might only be short-term.

14.3 Preparation of Records

- Staff should ensure that records selected for digitisation are physically suitable for scanning. This includes the removal of staples and paper clips, replacing documents with copies where tears and creases may impact quality, and ensuring that any attachments are properly identified;
- Where possible, records such as maps and plans should be scanned at their original size. Where such documents are resized, the source record must be retained for the full duration of its retention requirements;
Audio visual records are typically stored on physical carriers such as DVDs, video tape, film, and cassettes. The carrier and media must be checked for damage prior to digitisation.

14.4 Creation of Metadata
- Appropriate metadata must be created for each record and captured in the University’s recordkeeping system or a suitable business information system.

14.5 Calibration and Choice of Equipment
Calibration is very important in digitisation projects in order to ensure that equipment is performing at a level that meets quality assurance and international standards.
- Scanning equipment should be selected according to the type of records being digitised and the specific purpose it is required to perform;
- Scanning equipment should be calibrated in accord with relevant industry and international standards;
- Calibration checks should be undertaken during the course of a digitisation project. The frequency will depend on the quantity of records that are scanned and the time period over which they are scanned;
- Calibration targets should include colour and density checks and fine lines for detail. Formal Calibration Test Targets are necessary for eliminating wide differentials in assessments of quality that typically result from subjective evaluations;
- Where digitisation projects are contracted to an external provider, the provider’s service must meet international standards;
- Data must be kept that shows that the scanning equipment was tested to meet these standards by way of resolution calibration test targets.

14.6 Use of Scanning Targets
- A colour or greyscale test target and measurement scale is required for each type of record that is to be scanned (e.g. maps, drawings, plans). This is to ensure that material may be colour and tonally corrected on a wide range of viewing environments and accurately reproduced to size.

14.7 Verification of the Digitised Record
Digitised records must be subjected to quality assurance procedures to ensure they are as authentic, complete, reliable and usable as the source records from which they were created.

If an electronic reproduction of a record is to be accepted as evidence in a court of law in place of the source record, the University must be able to demonstrate that the digitised version is as authentic, complete, reliable and usable as the source record from which it
was created. The University must therefore be able to show that written procedures were followed and quality assurance checks performed that established the integrity, authenticity and completeness of the digitised records.

- Digitised records must be checked to ensure that the source record has been completely digitised;
- Checking should preferably be undertaken by a second staff member;
- Source records should be re-digitised where necessary.

14.8 Retention Periods

- A minimum retention period must be identified for all records selected for digitisation;
- Where the minimum retention period of the records is longer than ten years the digitised version must be converted or saved in an approved long-term file format as specified in the SRO-issued Digitisation Specification;
- Where the minimum retention period of the records is less than ten years the digitised version may be saved in any file format;
- As with all electronic records, the University is required to monitor digitised records and ensure they remain accessible for their full retention period;
- Digital file formats exist in a dynamic environment and digitised records with long-term retention requirements must be migrated into upgraded or alternative formats to ensure their ongoing preservation and usability. Refer 11. Data Migration.

14.9 Destruction of Source Records

Following their digitisation, source records may only be destroyed in accordance with the requirements of the General Disposal Authority for Source Records. Destruction of source records is only permitted if all the following conditions are met:

- Digitisation processes must meet the minimum compliance requirements of SRC Standard 8 Managing Digital Information – Principle 5 Digitisation; and
- File formats of the reproductions must meet the requirements of the Digitisation Specification; and
- Reproductions must be registered or captured in the University’s records management system or incorporated into a business information system at the time of digitisation; and
- Reproductions must be quality-tested and meet the required degree of authenticity, integrity, reliability and usability necessary to substitute for the source records for the purpose for which the source records were created or kept; and
- Source records must be identified in, or covered by, an approved disposal authority; and
• The reproductions must be kept and be accessible for as long as required under the relevant approved disposal authority.

14.10 Source Records Retention Periods

Source records must be retained for an appropriate period of time after their digitisation for quality control and risk management purposes. The following requirements apply:

• Routine, high volume administrative ‘transactional’ records such as purchase orders, invoices and receipts may be destroyed once the accuracy and integrity of the reproduction has been verified;

• All other source records must be retained for at least 6 months before being destroyed to ensure that:
  ▪ Digital reproductions have been created in accordance with the Digitisation Specification; and
  ▪ All quality control and assurance procedures and checks are successfully completed; and
  ▪ Re-digitisation of the source records has been undertaken where needed.

14.11 Source Records that must not be destroyed

Destruction of source records is not permitted under the following circumstances:

• When the records are State archives which were created before the year 2000. In this situation, the original records must be retained by the University as State archives until they are transferred in their original format to the State archives collection, or retained by the University under SRC Standard 7: State Archives Retained by Government Organisations;

• When the records have significant aesthetic or intrinsic value in their original format;

• When the records are subject to a legislative or Government requirement that the original record format be kept;

• When the records are State archives which are on loan to the University from the State archives collection;

• When the records are not identified in, or are not covered by, an approved retention and disposal authority.
15. Retention and Disposal

15.1 Overview

Staff are responsible for retaining and disposing of the University’s records in accordance with legislative requirements, government regulations, and the Murdoch University Recordkeeping Policy.

Records must be retained for varying periods of time in order to satisfy various legal, fiscal, administrative, and archival requirements. Retention periods for specific records series are shown in disposal authorities authorised by the State Records Commission.

Retention periods are measured in years or semesters following the occurrence of a specified event such as the end of a financial or calendar year, the end of a specified appeal period, the completion of an audit by the Auditor General or the discharge of a loan.

Most records will eventually be destroyed. However, records with long-term, historical value to the University, political scientists, scholars and historians must be retained permanently. The State Records Act 2000 refers to these records as State Archives because of their long-term significance to the State of Western Australia. Archival records are identified in the disposal authorities.

15.2 Disposal Authorities

Staff must refer to the General Disposal Authority for State Government Information (GDASGI) published by the State Records Office and the Western Australian University Sector Disposal Authority (WAUSDA) when appraising records for disposal.

The General Disposal Authority for State Government Information includes records that cover administrative, financial and human resource records common to most organisations.

The Western Australian University Sector Disposal Authority is a systematic listing of records series relating to the core functions of universities that are not adequately covered by the GDASGI.

These disposal authorities provide staff with a legal and authoritative basis to dispose of records. Adherence to them will assist staff in the ongoing management and timely disposal of records and help to ensure the University’s compliance with its legislative environment.

Staff involved with disposal activities should be reasonably acquainted with the introductory notes in the disposal authorities.
15.3 Disposal of Records

Retention and disposal authorities specify the minimum retention periods that must be observed before records can be legally destroyed. Therefore, records may be retained for a longer retention period than shown in the disposal authorities but they must not be destroyed prior to the retention periods indicated in the authorities.

All records must be appraised for possible archival value and historical significance to the University. These records must be retained permanently as State archives.

It is good practice for Offices and Schools to conduct periodic reviews of their recordkeeping systems in order to prevent the accumulation of records and the inappropriate reference to records that are no longer relevant or required to be kept. This not only facilitates the efficient retrieval of relevant documents but also ensures that limited storage space is responsibly managed.

All records of a confidential and sensitive nature must be disposed of in confidential and secure waste bins provided by the Development and Commercial Services Office.

15.4 Authority to Destroy Records

The authority to sign off on the destruction of records resides with the University’s Chief Executive Officer, the Vice Chancellor. This authority is delegated to the Manager, Records Management & Archives in accordance with the powers vested in the Vice Chancellor under s.3(a) Statute No. 25 Vice Chancellor.

15.5 Copies of Records

A copy of a record may be destroyed at any time without reference to the disposal authorities once its reference value has ceased, and where the official version of the record is verified as being already included in a recordkeeping system of the University. For example, Offices and Schools often keep copies of official records that are held on the staff files managed by the People and Culture Office. These records can be destroyed as soon as their reference value has ceased and without the requirement to refer to the retention and disposal authorities.

Copies of records should be managed according to the following guidelines:

- Exact copies of records can be destroyed at any time;
- Copies of documents that contain significant additional information not shown on the original, such as authorisations and handwritten annotations that elaborate on a matter of some significance, should be retained as official records;
- Copies of documents, such as committee minutes, distributed for information purposes only can be destroyed once their reference value has ceased;
- Data held in backup media for disaster recovery purposes is a copy of data held in electronic systems and can be erased once its purpose has been served.
15.6 Draft Documents and Working Papers

Where a final version of a document exists, any previous versions and working papers can generally be destroyed once their reference value has ceased. However, previous versions and working papers that contain significant information not found in the final version of a document should be retained as official records and should only be destroyed in accordance with authorised disposal authorities.

As per item 4.6, drafts and working papers should be managed according to the following guidelines:

- When a document has been finalised any previous versions, working papers, rough calculations and background notes can be destroyed once their reference value has ended. These records serve a facilitative purpose and consequently have a temporary usefulness which typically ends once a document has been finalised;
- Drafts and working papers that contain significant information not found in the final version of a document should be retained as official records;
- Working papers relating to the development of University policies and standards should be kept where they provide useful background information;
- Working papers and previous versions of legal agreements, contracts, policies and other significant documentation should be retained where there is a requirement to demonstrate the evolution of a matter and how key decisions were reached.

15.7 Ephemeral Records

Ephemeral records are records that only need to be retained for a very limited period of time. These records have little, if any, value to the University and can be destroyed at any time without reference to the disposal authorities. They include announcements of social events, leaflets, flyers, copies or extracts of documents sent only for reference, personal communications, catalogues, brochures, and copies of publications received from other organisations such as annual reports and newsletters.

15.8 Freedom of Information, Litigation, Investigations, and Audits

Any records relevant to legal processes such as discovery and subpoena or required for internal or external review or investigation or relevant to an application made under the Freedom of Information Act 1992 or any subsequent reviews by the Information Commissioner must not be destroyed until action has been completed even if the retention period has passed.

15.9 Procedures for the Disposal of Records

Written authorisation to dispose of records must be obtained from the Manager, Records Management & Archives.

The preparation and authorisation of formal disposal lists supports organisational accountability and transparency by demonstrating that the University’s records have
been disposed of in accordance with authorised disposal authorities and government regulations.

The following guidelines will assist staff in following correct procedure for the disposal of records:

- Identify records for disposal;
- Set aside any records with potential long-term historical value and liaise with the Records Management & Archives Office concerning their transfer to the University Archives;
- Use the ‘Records Disposal List Form’ to prepare a listing of records to be authorised for disposal in accordance with the disposal authorities;
- Consult the General Disposal Authority for State Government Information and the Western Australian University Sector Disposal Authority to determine disposal action for the records;
- Completed Records Disposal List forms should include a description of the records identified for disposal, the dates covered by the records, the format of the records, and the disposal date and disposal authority reference numbers that are applied to the records;
- If a record fits into more than one class of records in the disposal authorities, always choose the longest retention period;
- If the disposal trigger has not occurred for some records, do not proceed with disposal for those records but set a future review date;
- Forward the ‘Records Disposal List Form’ and a signed ‘Records Disposal Authorisation Form’ to the Manager, Records Management & Archives once it has been authorised by the appropriate Head of Office or School;
- The list of records identified for disposal will be reviewed by the Manager, Records Management & Archives. Disposal action may be undertaken once written authorisation is received.

15.10 Scope of Disposal Authorities

The disposal authorities cover all records irrespective of format. This includes hardcopy and electronic records maintained in computer systems including databases, spreadsheets, websites, records created by electronic mail systems, and records stored on microfiche, CDROM and in electronic filing systems.

The disposal authorities apply to all records created and received by staff at the Murdoch, Rockingham and Mandurah campuses, and all Centres and Institutes.

The disposal authorities do not apply to records created by associated organisations of the University or to the Guild of Students.
15.11 **Penalties**

An employee who destroys a record outside the authorisation of the above disposal authorities commits an offence under section 78(3) of the *State Records Act 2000* and risks a (maximum) penalty of $10,000.

15.12 **Review**

As required by section 28(5) of the *State Records Act 2000*, the *Western Australian University Sector Disposal Authority* will be reviewed periodically for currency but not later than 5 years after the last approval date by the State Records Commission.
16. Archival Records

16.1 Role of the Murdoch University Archives

On 15 November 1991, Murdoch University wrote to the Library Board of Western Australia requesting permission to manage all the University’s archives onsite under Section 26(1) of the Library Board of Western Australia Act 1951-1983.

At its meeting held on the 18th February 1992 the Library Board of Western Australia authorised Murdoch University to establish a purpose-built Archives facility under section 26(1) of The Library Board of Western Australia Act 1951-1983. Under this agreement, the University is authorised to manage and retain custody of all the archives of the University while under the professional care of the Records Manager & Archivist.

Subsequently, the Murdoch University Archives was established in 1992 for the purpose of collecting, preserving, managing and making available for reference use those records of the University designated as having archival value. The records are to be made available for the benefit of the University and the broader community.

The Murdoch University Archives facility was purpose-built to provide a suitable environment for the storage and preservation of the University’s archival records. The facility is constructed and fitted according to archival standards and meets the requirements of statutory Standards, Guidelines and Directives.

16.2 State Archives

State archives are records that must be retained permanently. They must be retained within an approved archival repository, this being the Murdoch University Archives facility.

Archival records are non-current records that have been selected for permanent preservation as a result of their significant administrative, financial, legal, or research and informational value. They comprise any medium that conveys information including correspondence, files, minutes of committee meetings, maps, plans, photographs, microfilms, audio-visual material such as audio cassettes, video and DVD, and memorabilia.

Archives have continuing historical significance to the University and/ or to political scientists, scholars, historians and the general community and regarded as an important part of the State’s cultural heritage. They include records that document the establishment of the University, the drafting of its legislation, major organisational decision making, significant projects, policy and procedures, minutes and agendas of the university’s major committees, photographs, and any records of historical significance.

Section 32(1) of the State Records Act 2000, requires the University to transfer its State archives to the State archives collection once they become twenty-five (25) years old. However, in accord with the State Records Office directive, electronic State archives are
to remain in the custody of the University and managed in accordance with SRC Standard 8 – Managing Digital Information.

16.3 Responsibilities

The Records Manager & Archivist has responsibility for the management of the University Archives collection, the development of policy and procedures, and for the exercise of the responsibilities outlined below.

- Consult with Offices and Schools to identify and protect State archives;
- Prevent the destruction of potential archival records by promoting quality records management practices throughout the University;
- Preserve the Archives collection. This includes ensuring the physical environment remains suitable for the long-term preservation of archival records; inspecting and selecting records for repair, and selecting records that should be reproduced for purposes of preservation;
- Appraise potential archival records for acquisition into the University Archives;
- Document meaningful descriptive information about archival records collected for the University Archives on the records management system;
- Organise the Archives facility including proper packing, labelling and arranging of archival records;
- Ensure archival records are identified in the Western Australian University Sector Disposal Authority;
- Respect the confidentiality of archival records to which privileged access is given;
- Accept only material that falls within the Collection Policy;
- Undertake regular inspections of the Archives facility to check for possible infestations of termites, cockroaches, spiders, silverfish, rats and mice and arrange periodic fumigation to protect the archive collections;
- Ensure that fire hazards are eliminated. This includes ensuring sufficient fire detection equipment, not permitting the cluttering of aisles, not storing highly flammable materials, not overloading electrical outlets, and ensuring archive boxes are stored more than 30cm from light fittings;
- State archives that have restricted public access must be identified and reasons provided for the restrictions and when they will cease.

16.4 Acquisition and Appraisal

The Records Manager & Archivist shall appraise all material against the Archives Collection Policy and SRC-approved disposal authorities. Care must be taken to avoid duplicating holdings by checking the Archives database and checking with the Library Special Collections for possible identical holdings.
All potential archives must be appraised on the basis of their evidential (primary) and/or informational (secondary) value. The evidential value of a record refers to the function a record had for the Office or person that created the record. It includes records that:

- have continuing administrative, legal or financial use;
- serve to protect civic, legal, property or other rights; and
- demonstrate the University’s historical development, structures, functions, policies and significant developments

16.5 Collection Policy

The Collection Policy refers to the scope and content of the records to be collected for the Murdoch University Archives. It broadly covers what the archives will collect, what the limits of the collection will be, and what types of material are of particular interest.

The University’s Collection policy includes records from:

- Administrative Offices
- Schools
- Murdoch, Rockingham and Mandurah Campuses
- Research Centres and Institutes of the University

The Murdoch University Archives shall collect and maintain records that have continuing administrative, legal or financial value or reflect the historical development and functions of the University. The following records shall be collected and preserved:

- Records that describe the University’s origins, structure, planning, purpose, and operations;
- Legal documents including property deeds and significant contracts;
- University legislation including establishment legislation, Statutes, Regulations and by-laws;
- Minutes, agendas and reports of major university committees including the Senate and Academic Council and their standing committees, and other significant committees;
- Financial records that document the conduct of the University’s financial affairs including financial statements and budgetary papers;
- Academic and strategic planning records;
- Reports including the Murdoch University Annual Report, and annual reports of Schools, research institutes and centres, and Research Reports;
- University publications including On Campus, Murdoch News, Synergy, Discovery, In Touch, and The University Handbook;
- Policy and procedure files;
• Records relating to significant functional reviews of organisational structures both Academic and Administrative;

• Records relating to final reports of significant reviews prepared by external organisations and where the University has made a significant submission to the review;

• Research, personal, and published papers of private persons associated with the University, including retired, resigned or deceased academic and administrative staff, Senate members and benefactors;

• Final reports of research grant files where the research project is of national or international significance and makes a substantial contribution towards the professional body of knowledge and/or has commercial and intellectual property spin-off;

• Records relating to the honouring of distinguished individuals and organisations by the dedication or naming of memorial plaques, benches, university buildings, lecture theatres or grounds in their honour;

• Newspaper clippings that feature articles about Murdoch University;

• Records relating to the election of the Chancellor;

• Records relating to the recruitment of the Vice Chancellor;

• Personal files of notable staff including Vice Chancellors, Deputy Vice Chancellors, Professors and other staff of note;

• Diaries of notable staff;

• Correspondence with significant historic value including correspondence with politicians;

• Documentation relating to major campus developments including new buildings and commercial developments;

• Postgraduate research student files;

• Architectural plans and drawings, and building specifications reports relating to University buildings and grounds;

• Photographs that have significant historical value to the University;

• Records including final reports that have significant historical value to the University submitted to government agencies;

• University statistics;

• Audio-visual recordings of graduation ceremonies, significant public lectures, and opening ceremonies;

• Significant memorabilia;

• Such other documents which, in the opinion of the University Records Manager &Archivist, are of archival value.
The collection policy shall not include records with short-term retention requirements, artworks, or material deemed unsuitable for storage because of its size or nature or because the Archives is not equipped to manage them.

The collection policy shall not duplicate holdings in the Library Special Collections.

16.6 Access and Control

- Access to the University Archives, and retrieval and refile of records, is limited to staff of the Records Management & Archives Office;
- Confidential records, or records transferred with restricted access provisions are only to be released with written permission of the donor, originating body or nominee, unless access is granted under the Freedom of Information Act 1992;
- Persons given access to archival records are required to respect ethical obligations of confidentiality and privacy;
- All records transferred to the University Archives are to be used in the Archives facility or in the Records Management and Archives office under the supervision of the Records Manager & Archivist, except School records which can be loaned for a limited, specified period to the originating School;
- Records borrowed from the University Archives, including records borrowed for litigation purposes, must be returned in their initial condition;
- Researchers are not to have access to storage areas and there shall be no open-shelf access;
- Records should be handled with care and should not be marked, altered or changed in any way or removed from the University Archives;
- Limited general reference assistance may be given by letter, email or telephone for specific enquiries, but it is not possible to carry out extensive research on behalf of researchers unable to visit the University Archives;
- In all cases where publications are based in part on research in the University Archival Collection, acknowledgment must be made by reference to the Murdoch University Archives and to the name of the particular collection used;
- Members of the public requesting access to university archival records are required to complete and sign a ‘Murdoch University Archives Access’ form. The Access Form must be approved by the Records Manager & Archivist. The Access Form requires the person’s name and address, reason for request, subject of records inquiry, and an undertaking to deposit with the University Archives for preservation in the Library, a copy of any work written or relevant part thereof, which quotes material from the University Archives or which is in any way dependent on them;
- A reasonable fee shall be charged for any photocopies made by the Records Management & Archives Office on behalf of the researcher, and at the discretion of the Records Manager & Archivist a reasonable fee shall be charged for time researching and copying;
• Repairs to damaged archives should not be attempted without first consulting the State Records Office.
17. Murdoch University History

17.1 Research and Promotion

The Records Management & Archives Office is in a unique position to promote an awareness and appreciation of the University’s history, its achievements and its contribution to the State’s heritage. The University’s history has value for the celebration of its anniversaries, Open Days, marketing, and for presenting a positive image to prospective students and maintaining links with its alumni and former staff.

The Records Manager & Archivist shall research the University’s history from source documents including original documentation and files in the University Archives, annual reports, Senate and Academic Council minutes, university publications, newspaper articles, university statistics, photographs, and library resources. Associations with staff with an interest in the University’s history shall also be fostered.

The following historical information shall be researched, developed and updated on the Records Management & Archives homepage:

- Graduation ceremony speeches including the Occasional Address, Valedictory Address, and honorary degree citations;
- Timelines that chronicle the University’s growth and achievements including, but not limited to, student enrolment numbers, list of former Guild Presidents;
- Information about Sir Walter Murdoch;
- Profiles of the University’s Chancellors, Vice Chancellors, Foundation Professors, and other persons of noted association with the University;
- Maintaining a listing of persons to have served on the University’s Senate, including the basis of their appointment and their term of office;
- Early history (establishment years) of the University including School histories;
- Key public lectures administered by the University including the Sir Walter Murdoch Lecture series, Keith Roby Memorial Lecture in Community Science, and other lectures deemed to have ongoing historical value;
- Newspaper articles particularly of the University’s early history. Their reproduction on the University’s website requires payment of a licence agreement with WA Newspapers Ltd arranged through their Events and Editorial Office;
- Student achievements including University Medallists and Rhodes Scholars;
- Staff achievements including the award of Senate Medals, and the Vice Chancellor’s Excellence in Research Awards;
- Photographs with historic value.
17.2 Murdoch University History Collection Advisory Group

The Records Manager & Archivist is a member of the ‘Murdoch University History Collection Advisory Group’. This is a university-wide advisory group established for purposes of providing a framework for the collection of materials that have historical significance for university celebrations and other activities and uses.

The role of the Advisory Group is to provide a forum for discussion about:

- Leading figures in the University’s History
- Art and architectural History (Landscape and grounds, buildings)
- Campus history (Perth, Rockingham, Mandurah, Singapore and Dubai)
- Historical photographs
- Oral histories
- Artefacts and memorabilia
- Ephemeral items

The Advisory Group operates within the framework of the Murdoch University Library Collection Development Policy.
18. Offsite Storage of Temporary Records

18.1 Introduction

To meet its storage needs for hardcopy temporary records, the University has contracted Iron Mountain Australia Group Pty Ltd as its offsite storage provider. Iron Mountain’s services are approved under Common Use Contract CUAREC2015 for the supply of ‘Storage, Retrieval, Destruction and Digitisation of Paper and Electronic Records’ approved by the Department of Finance on 15 July 2015.

Murdoch University Account details:
Account Name: Murdoch University (61151)
Level 1 Account Number: RL501676
Level 2 Account Number: 61151
Level 3 Account code: L&G/OHR etc.

Hence Customer account number: RL501676/61151/L&G

Iron Mountain use a web-based ordering system for placing requests for the retrieval of archive cartons.

18.2 Numbering System

At the start of each calendar year, it is necessary to create new record numbers in the records management system for cartons of records that will be transferred to storage during the coming year. This will be the ‘container number’ that is used for cartons sent offsite.

The numbering pattern is to include a prefix that identifies the year the cartons were sent offsite. For example, in 2018 the numbering pattern will be 18/1, 18/2, 18/3 and so on. The title of each carton will be ‘Offsite storage box 2018’ for all records created in 2018.

It is recommended that 400 records be initially created and any new numbers may be created later as required. The 5-year average number of cartons transferred to storage 2013-2017 is 465 cartons.

The default setting for offsite storage boxes is set as “offsite storage”.

18.3 Receiving Records from Offices and Schools

The following procedures are to be observed by Offices and Schools when records are transferred to the Records Management & Archives Office for storage purposes:

- Staff must first consult retention and disposal authorities authorised by the State Records Commission to determine whether any records can be immediately destroyed and do not need to be sent to the Records Management & Archives Office. Refer s. 15 Retention and Disposal;
• Staff must liaise with Records Management & Archives before any cartons are transferred as it is necessary for Records staff to ensure that sufficient space exists before accepting large shipments of cartons;

• Staff should advise the quantity of boxes and provide a description of the contents and the dates covered by the records;

• Staff should contact the Development and Commercial Services Helpdesk to arrange collection and transfer of cartons to the Records Management & Archives Office;

• After receiving the cartons, Records Management & Archives staff will process the records for transfer to storage. Records must be examined for any possible archival value;

• Industry-standard, archive cartons must always be used. Photocopy paper and boxes used for packing stationery supplies must not be used. The offsite storage provider has instructed its courier to reject inappropriate cartons. A re-packing fee will be incurred by the University when records are re-packed by Iron Mountain staff;

• Staff should take care not to over-pack cartons particularly with heavy items such as books and diaries. Cartons weighing in excess of 16kg will not be collected because of occupational health and safety regulations.

18.4 Preparing Cartons for Transfer to Storage

(a) Enter the following information about each carton in the records management system:

(i) **Descriptive information** - information about the contents of cartons transferred to offsite storage must be provided for reasons of accountability and to ensure that records can be retrieved when needed at a later date;

(ii) **Retention period** - a retention period for each carton must be provided:

   • consult authorised disposal authorities,
   • write the year of disposal on an adhesive label and affix to the carton,
   • enter the year of disposal in the records management system,

(iii) **Security level** - the security level in the records system must be set at ‘Restricted Access’ for all personal and confidential records. The ‘General Access’ security level may be used for all other records;

(iv) **Container (carton) number** - enter the Container number and tick the ‘Enclose the Record Now’ check box;

• Apply **Radio Frequency Identification Technology (RFID)** tags to each carton according to their relevant cost centre;

• Open the ‘Cartons with Recall’ **Excel spreadsheet** and enter the carton number, cost centre details, destroy year, and the RFID tag number for each carton;
• Provide Iron Mountain with details of the new carton additions by completing a “New Item Registration Form”. Use a separate form for each cost centre. The form requires the RFID tag number, the University’s alternate code and a destruction review year for each carton. The alternate code is the archive box (container number) that is used when making requests for carton retrievals. The forms should be emailed to resource.wa@recall.com;

• Request collection of the cartons by Iron Mountain by selecting ‘Collect from me’ and specifying the number of cartons. Note: a separate request is required for each cost centre. Ensure the cartons are arranged for collection according to the cost centre of each carton;

• The courier will scan the RFID tag of each carton and provide a printout of the cartons collected. File the printout for future reference as it will be required in order to clarify any issues that may arise when the cartons are uploaded at the warehouse;

• Update the Excel spreadsheet with the date the cartons are collected.

18.5 Retrieving Cartons from Storage

Orders are placed via Iron Mountain’s web-based ordering system.

The University’s level 1 Account Number is RL501676. The Level 2 account number is 61151. Level 3 numbers are the cost centres, e.g. OHR, L&G.

From the menu select ‘Work Orders’. The default selection is ‘New Order - Deliver to me’.

Where: This screen provides default information at the level 1 and 2 fields and also the delivery address. Select the relevant level 3 cost centre and then click ‘Search for items to be Retrieved’.

What: The default setting is the University’s ‘Alternate Code’, this being the carton container number. All codes must be preceded by the cost centre. This is accessed from the Excel spreadsheet ‘Cartons with Recall’. For example, L&G/16/232. Alternatively, the ‘Iron Mountain Bar Code’ may be selected.

Click ‘Go’ and then click the ‘Retrieve Box’ when the search results are displayed. Then select ‘Add Selected Items to Cart’. Repeat this step if more than one carton from the same cost centre is required. Then select “Checkout”.

When: Select an option for the courier service. The default option is routine delivery. Enter the name of the staff requesting the carton/s and the cost centre and click ‘Send Order to Iron Mountain’.

• Routine Delivery – the order must be placed by 3pm for delivery by 12pm the next business day.
The maximum number of cartons that may be requested for delivery by routine delivery is 50 items.

- **Priority Delivery** – the order must be placed before 10.00am to be delivered on the same day and by 5.00pm. If the order is placed after 3.00pm it will be delivered the next business day by 5.00pm.

  The maximum number of cartons that may be requested by priority delivery is 25 items.

- **Urgent Delivery** – the order must be placed by 3pm for delivery within 3 hours on the same day. Orders placed 3pm-5pm will be delivered the next business day by 11am.

  The maximum number of cartons that may be requested by urgent delivery is 10 items.

**Finish:** Select ‘Send Order to Iron Mountain’. A prompt will request confirmation to send the order. Select the option to receive an email notification confirming the order.

Email may be used when the Iron Mountain portal is unavailable.

### 18.6 Permanent Retrieval
Select ‘Permanent Retrieval’ when a carton needs to be permanently retrieved. A special fee will be incurred but the University will no longer incur a monthly fee for the carton’s storage.

### 18.7 Amending an Existing Work Order
Any changes to an existing work order must be submitted by email.

### 18.8 When a Requested Carton is Delivered
Once a carton/s has been delivered, remove the documents/files that were requested and apply an ‘Offsite Storage’ adhesive label and ‘Archive carton No.’ label. Attach a note to the archive carton that indicates the record/s borrowed, by whom and the date. Enter borrower details in the records management database.

### 18.9 Returning Cartons to Storage
When records have been returned to the cartons, they can be returned to offsite storage. To minimise courier collection fees it is advisable to arrange this service only when the number of cartons reaches around 40 cartons.

### 18.10 Ordering New Cartons
To order archive cartons from Iron Mountain, select ‘Search for items to be Retrieved’ and from the next screen select ‘Order Supplies’.
The re-order code for large two-piece cartons is S7030 Business cartons. The re-order code for small one-piece cartons is S8020 Legal cartons. Cartons are supplied in quantities of twenty-five cartons. Therefore, the quantity to be requested will be ‘1’ for 25 cartons and ‘2’ for 50 cartons.

18.11 Cost Centres

The following are the cost centres in use as at November 2017:

Level 3 cost centres under RL501676/61151
- Admissions and Recruitment Support (PS&AC)
- Campus Operations and Services (CS)
- External Engagement (TE)
- Marketing and Communications (CC)
- People and Culture Office (OHR)
- Research and Innovation (R&D)
- School of Business and Governance (MG)
- School of Education (EDU)
- School of Engineering and Information Technology (ENG)
- School of Health Professions (HP)
- School of Law (LAW)
- School of Veterinary and Life Sciences (VET)
- Student Centre (SC)
- Student Services (CSA)
- University Secretary’s Office (L&G)
- Vice Chancellor’s Office (VC)

Level 3 cost centres under RL501676/61151R
- Student Life and Learning (CSA)

A request should be made to Iron Mountain when the name of a cost centre has changed. This ensures the correct name is shown on the monthly invoice. Note: Iron Mountain cannot change the original acronym that was used when setting up a cost centre, e.g. L&G (and which forms part of the carton number), but only the title of a cost centre.
18.12 Destruction of Cartons

Iron Mountain provides a secure destruction service on behalf of the University.

The University is notified via a hardcopy Item Retention Review notification. This report lists cartons that are scheduled to be destroyed according to the destruction dates previously advised by the University when submitting new items listings. The destruction dates must be reviewed and a new destruction date determined where required.

Upon receipt of the destruction request, Iron Mountain will raise a destruction order and email a copy of the preliminary work order for verification and final authorisation. On receipt of authorisation the destruction order will be activated and advice sent on when the cartons are to be destroyed.

The ‘destroy’ field in the ‘Cartons with Recall’ Excel spreadsheet must be completed for each carton.

A fee is incurred for the destruction of cartons. It is charged against the relevant cost centre and will appear on the monthly invoice.

18.13 Invoicing

A consolidated monthly invoice for each cost centre is provided to the Records Management & Archives Office.

The University is charged a monthly storage fee for each carton. Note: the rental charge for carton retention is for the month in advance.

Fees are also made for any services performed by Iron Mountain including courier fees for the collection and delivery of cartons, a carton retrieval and refile fee, and fees for the lodgement of new cartons.

Authorise payment after the invoice has been checked. Photocopy the invoice for reference purposes and forward the original to the University Secretary’s Office for payment.

When new carton additions are shown on the invoice under the generic heading ‘Murdoch University’, it will be necessary to request transfer of the new additions to the appropriate cost centre as advised in the New Item Registration Form that would have been submitted earlier.