INFORMATION MANAGEMENT

Procedure Manual

adelaide.edu.au

Table of Contents

Purpose 1

Acknowledgement 1

Further assistance 1

1. Introduction to information management 2

1.1 What is an 'information asset'? 2

1.2 What is 'information management'? 2

1.3 The University's policy on information management 3

1.4 The importance of good information management 4

2. Responsibilities for information management 4

3. Compliance requirements relating to information management 4

4. Lifecycle management of information assets 5

4.1 Govern 6

4.1.1 Strategy and planning 6

4.1.2 Leadership, sponsorship and investment 6

4.1.3 Roles, responsibilities and structures 6

4.1.4 Risk assessments 7

4.1.5 Compliance and performance monitoring 7

4.1.6 Quality assurance 8

4.1.7 Training 8

4.2 Plan & design 9

4.2.1 Business systems 9

4.3 Create/Receive 10

4.3.1 When and why to create information assets? 10

4.4 Organise 11

4.4.1 Capture 11

4.4.1.1 When to capture information assets? 11

4.4.1.2 What information assets need to be captured? 11

4.4.1.3 Where to capture information assets? 12

4.4.2 Manage metadata 12

4.4.3 Ensure information assets are reliable 13

4.4.4 Ensure information assets are findable 14

4.4.5 Store 14

4.4.5.1 Storing active information assets 14

4.4.5.2 Long-term storage 15
4.5 Use & Re-Use 15
4.5.1 Manage access – the basics 15
4.5.2 Privacy, confidentiality and other limits on access 16
4.5.3 Information classification 17
4.5.4 Security 17
4.5.5 Cyber security 18
4.5.6 Public Access 18
4.5.6.1 Freedom of Information (FOI) 18
4.5.7 Research Data 19
4.5.7.1 Open Access 19
4.5.7.2 FAIR Data Principles 19
4.5.8 Remote use of information assets 19
4.5.9 Business intelligence and analytics 19
4.6 Dispose 20
4.6.1 Disposal schedules 20
4.6.2 Disposal in the digital environment 20
4.6.3 Making disposal decisions 21
4.6.4 Destruction of temporary value information assets 21
4.6.5 Normal Administrative Practice (NAP) 22
4.6.5.1 The NAP test 22
4.6.6 Information assets required for legal purposes, inquiries and/or investigations 23
4.6.7 Decommissioning of business systems and websites 23
4.6.7.1 Business systems 23
4.6.7.2 Websites 24
4.6.8 Archives 24
Attachment 1: IM Compliance 26
Attachment 2: IM Roles & Responsibilities 27

Purpose

The *Information Management (IM) Procedure Manual* has been developed to support and supplement the University's *Information Management Policy*.

The *IM Procedure Manual* includes guidance and instruction for all Personnel[i] specific to the University context.

This Manual also provides references to additional resources and related University policies that Personnel should familiarise themselves with in order to have a full understanding of information management responsibilities and requirements.

Further, this Manual indicates where particular business areas of the University, such as the University Library and ITDS, have oversight or responsibility for assisting Personnel and local areas with particular aspects of managing information assets.

Acknowledgement

The *Information Management Procedure Manual* replaces the University's *Records Management Handbook*, although advice from the previous handbook that is still relevant has been included in this document.

The information management policies of other GO8 Universities have been taken into consideration and referenced during the development of this Procedure Manual.

Government standards and policy documentation have also been referred to and adapted as needed for the purposes of this Procedure Manual, eg State Records of South Australia's *Information Management Standard*, the New South Wales Government's *Information Management Framework* and related policies and guidelines, State Archives and Records Authority (SARA) of New South Wales suite of recordkeeping advice, and National Archives of Australia's information management standards and policies.

Further assistance

For advice, support and assistance in implementing and complying with the *Information Management Policy* and *Information Management Procedure Manual* contact the University Library - Special Collections, Archives and Recordkeeping.

1. Introduction to information management

1.1 What is an 'information asset'?

Within the University context, an information asset includes information, data and records in any format, where it is created or received through the conduct of University business and treated as an asset and resource that the University harnesses to meet its strategic, operational and legal needs.

An information asset may include, but not be limited to, written or electronic documents, records, publications, web pages, emails, text messages, spreadsheets, photographs and images, databases, tools and applications, drawings, plans, sound and video recordings, etc.

Information assets provide evidence of the University's research, academic, operational and engagement activities.

Research

- Risk Management & Data Management Plans
- Grant applications
- Funding requests & approvals
- Contracts & agreements
- Ethics applications & approvals
- Correspondence
- Lab & field notebooks
- Data – primary research, derived, analysed, published
- Questionnaires, surveys
- Models
- Test responses
- Slides, specimens & samples
- Project files
- Master lists
- Signed consent forms
- Research project financial management records
- Regulatory reporting records
- Technical & research reports
- Theses, research journals, scholarly articles & books/publications
- IP and commercialisation records

Academia

- Student information/records – admission, enrolment, academic progress, financial administration, graduation, discontinuation
- Student exams & assessments
- Curriculum development & delivery – University calendars, course outlines, etc
- Learning & Teaching materials – lecture notes, resources

Operations

- Correspondence – emails, letters
- Reports
- Briefing notes
- Memos
- Plans – operational, strategic
- Meeting agendas & minutes
- Working papers
- Agreements, tenders & contracts
- Asset management records
- Financial records – reports, receipts, invoices, budgets, estimates, statements
- Staff records – recruitment records, employment contracts, evidence of qualifications, appointments & reassignments, travel arrangements, compensation claims, training, counselling, discipline, etc
- WHS records – accidents & incidents reporting, inspection and audit reports, etc
- Policies & procedures

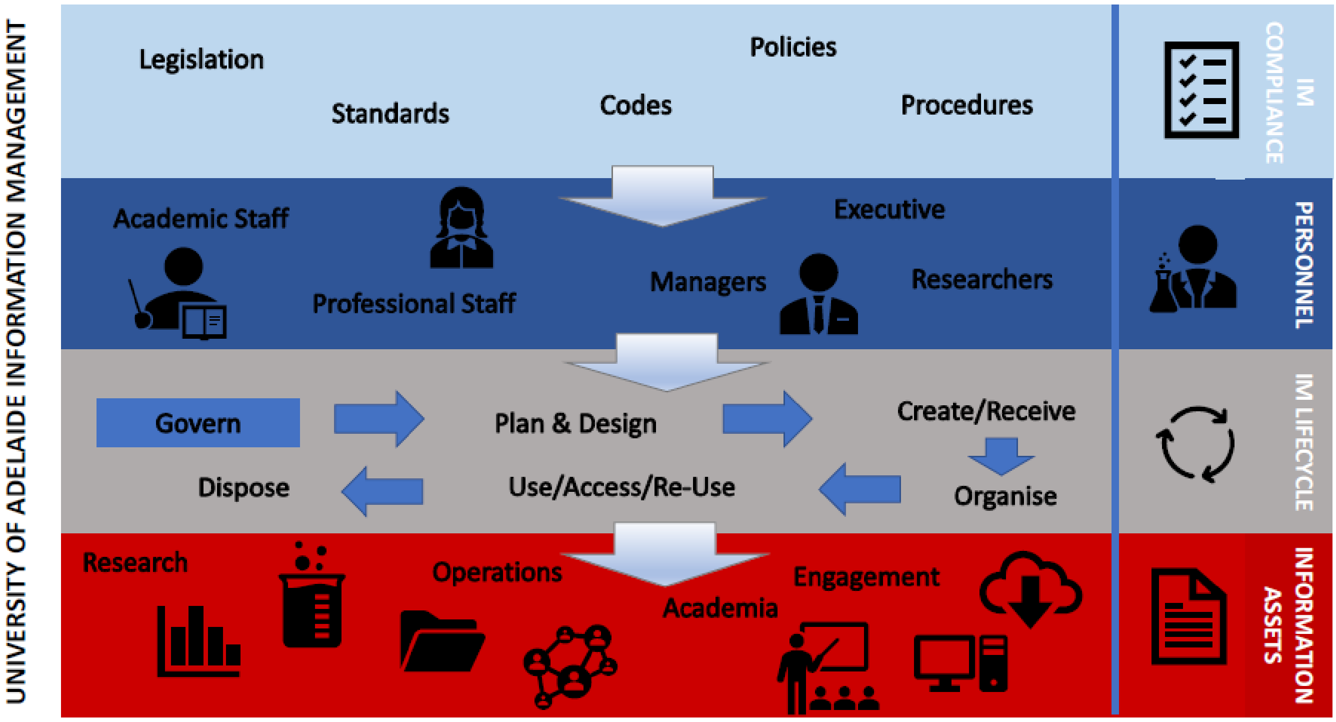
Engagement

- Marketing and events records
- Social Media – blogs, vlogs, reactions to posts, tweets, comments
- Website
- Addresses & presentations
- Media releases
- Public reaction – suggestions, complaints, congratulations
- Alumni relations

1.2 What is 'information management'?

Information management includes the structures, systems, people and processes to capture, manage, preserve, store and deliver the right information to the right people at the right time regardless of location. Information is delivered through multiple channels and interfaces and is managed throughout its lifecycle regardless of its source or format.

Effective information management relies on compliance, all University Personnel and the lifecycle management of information assets.



1.3 The University's policy on information management

The University's *Information Management Policy* outlines five principles:

- the University has a fundamental obligation to proactively manage its information as business-critical assets
- the University ensures responsibility for managing Information Assets is clearly assigned and documented
- the University creates and retains its Information Assets to meet accountability obligations and mitigate risk
- the University relies on its Information Assets to document, support and substantiate business decisions and outcomes
- the University effectively balances the disclosure of Information Assets with the need to maintain confidentiality as required.

All Personnel need to read the short Policy and be familiar with its contents, including:

- University officers appointed under the *University of Adelaide Act 1971*
- external members of the governing body
- any members of a committee of the University of Adelaide Council
- academic and professional staff
- titleholders, adjuncts, academic visitors and affiliates of the University
- researchers (including Higher Degree Research (HDR) students)
- contractors and consultants
- volunteers.

Any questions about the Policy should be directed to the University Library - Special Collections, Archives and Recordkeeping (SpARK).

1.4 The importance of good information management

Well-managed information is a valuable asset that contributes to the University's research, academic, operational and engagement activities through:

- supporting efficient business and the delivery of quality programs
- informing decision-making
- demonstrating accountability, integrity and transparency
- complying with mandatory laws and best practice codes
- enabling digital transformation
- assisting to mitigate risks
- protecting rights and entitlements
- adding economic value
- safeguarding reputation
- maintaining a reliable 'institutional memory'.

Implementing good information management will benefit University outcomes by enabling Personnel, divisions, faculties, schools, controlled entities and administration areas more broadly to:

- document all needed information about a person, decision, fact or event
- make sound decisions based on timely access to reliable University information
- share knowledge easily and avoid duplicated effort
- improve efficiency by leveraging opportunities provided by evolving information technologies
- protect and secure information
- know who has seen, changed, or removed University information when required
- retain trust and transparency by being able to account for actions undertaken, advice given and decisions made
- maximise return on investment by providing meaningful datasets to assist the University, its partners and the community, to use and reuse information
- create and preserve information that will contribute to the story and history of the University, its Personnel and students.

2. Responsibilities for information management

Responsibility for managing information assets is cascaded down throughout the University.

Specific responsibilities have been outlined in the *Information Management Policy* and are further explained in Attachment 2.

3. Compliance requirements relating to information management

As a publicly-funded institution operating in a heavily regulated and highly competitive environment, the University as an institution is expected to be compliant and accountable to an increasing number of external agencies and bodies, and to the public community it serves.

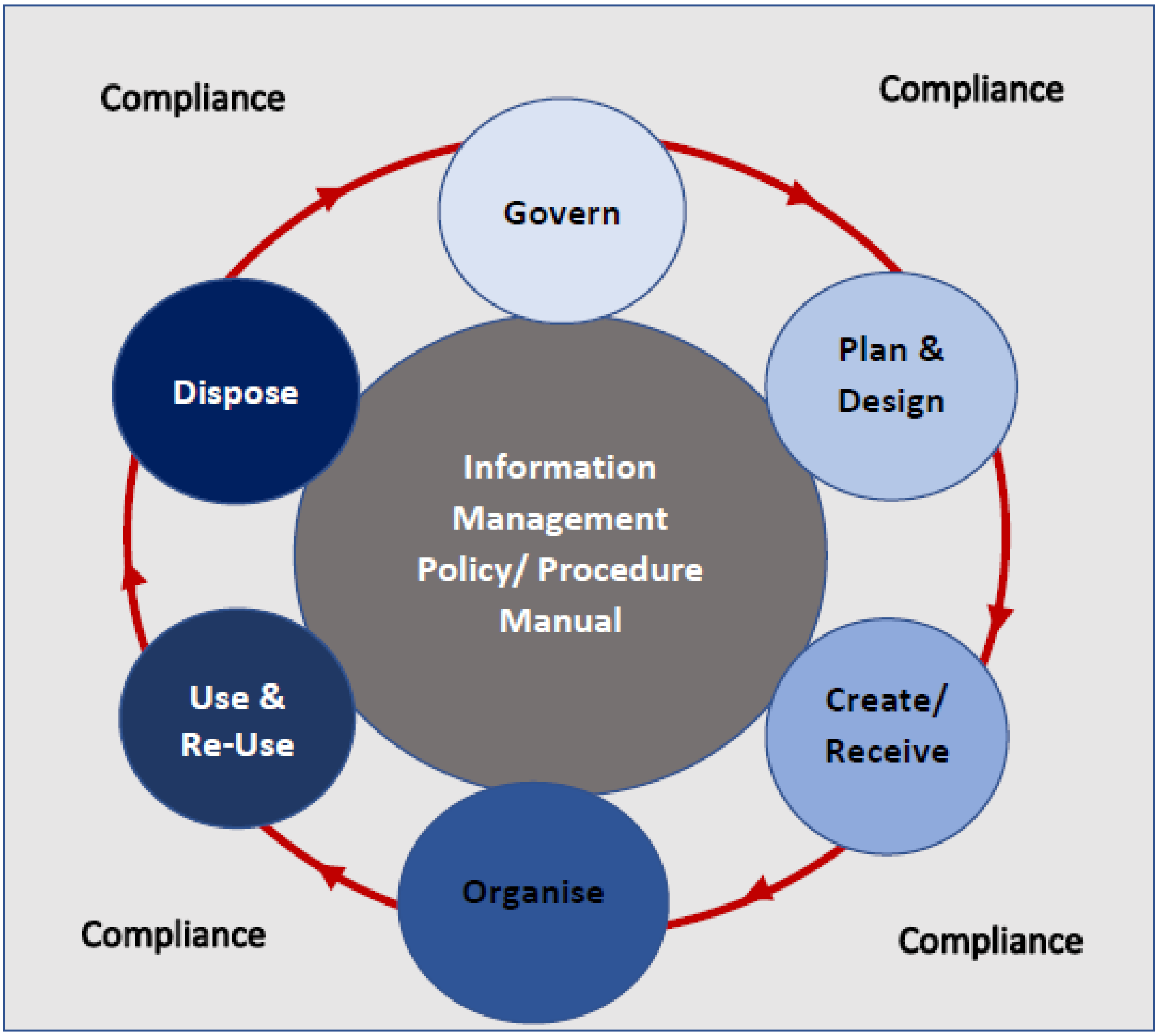
The University's compliance obligations arise from several sources, including legislation, mandated standards and contracts.

The major obligations, which are relevant to all University Personnel and information management, are shown in Attachment 1, with links provided for further information.

4. Lifecycle management of information assets

Lifecycle management aims to reduce inefficiencies and ensure the maintenance and protection of information assets for as long as they are required. It includes:

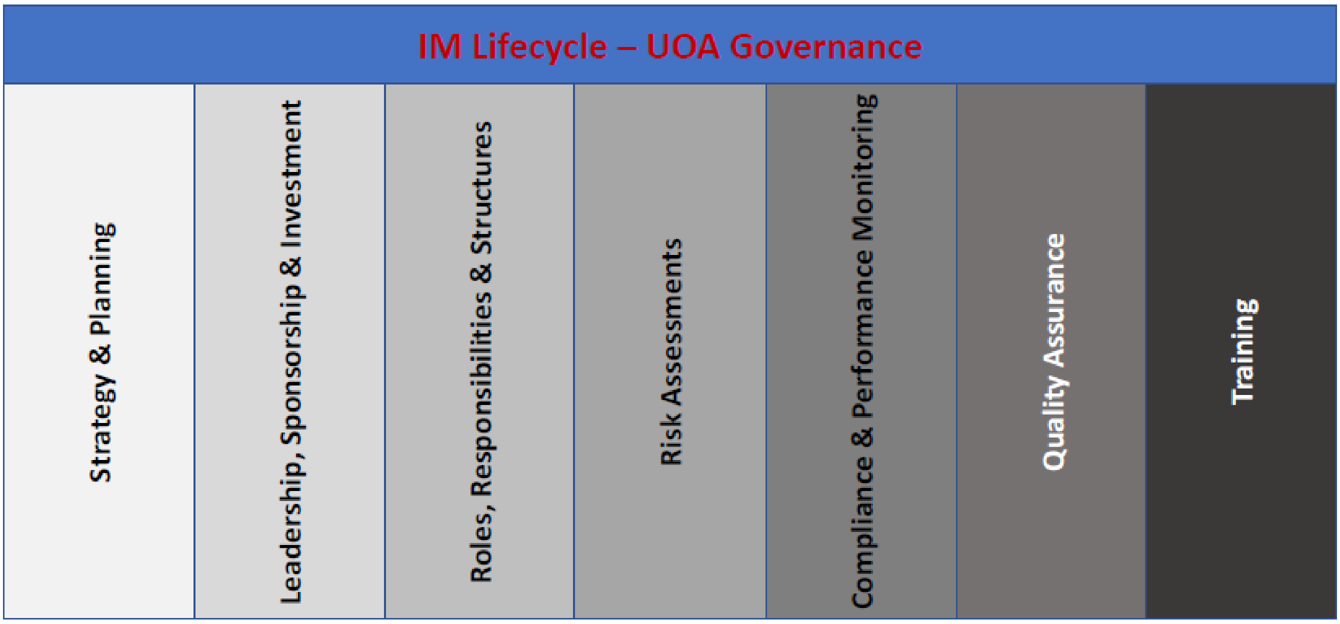
- **Govern** – governance framework, including leadership, monitoring, auditing/assessments, quality assurance and training
- **Plan and design** – includes developing and/or implementing business systems
- **Create/receive –** the creation, receipt or collecting of information assets
- **Organise** – capture, metadata management, reliability, findability, storage
- **Use & Re-use** – access, sharing, re-use, information classification, security, rights management, business intelligence & analytics
- **Dispose** – retention or destruction, migration, decommissioning of business systems, archives.



4.1 Govern[ii]

Governance addresses how the University's information assets are strategically managed to support decision making, research, learning and teaching, operations and engagement activities.

Good governance includes:



IM Lifecycle – UOA Governance

Strategy & Planning

Leadership, Sponsorship & Investment

Roles, Responsibilities & Structures

Risk Assessments

Compliance & Performance Monitoring

Quality Assurance

Training

4.1.1 Strategy and planning

Information management needs to be informed by strategic direction and planning to ensure information remains a valued, managed and business-aligned strategic asset.

Strategic direction will be provided by the University's Information Management Governance Committee, with reporting to the Vice-Chancellor Executive Group.

Planning by the *Information Management Roadmap* and the University's *Digital Future Technology Strategy* will align systems, services, processes, capabilities and requirements to support information creation, management, use and disposal.

4.1.2 Leadership, sponsorship and investment

Leadership, advocacy and funding need to be defined and allocated to enable delivery of information management objectives and outcomes.

In accordance with the *Information Management Policy*, Executive Deans and Divisional Heads are responsible for ensuring adequate resources are available to implement both the policy and this manual.

4.1.3 Roles, responsibilities and structures

Roles, responsibilities and business structures need to be defined and designed to support key University information management accountabilities, risks, deliverables and performance.

Refer to *Responsibilities for Information Management* for further details.

4.1.4 Risk assessments

Risk assessments inform the ongoing effective performance of information management. Risk assessments identify, evaluate and mitigate the risks around information and manage threats to its integrity, security, availability, longevity and useability in different environments and program or service offerings.

As a starting point, an information management risk assessment includes:

- reviewing the functions and responsibilities of business areas and determining related high-risk business processes and the information assets created as part of those processes and
- identifying areas of possible risk of information management failure, such as failure to create necessary information assets or unauthorised disposal.

An initial assessment will be the starting point for identifying performance objectives, determining what performance measures the University will need and what mitigation strategies need to be put in place for information risks.

The assessment will be scheduled and coordinated by the University Library - Special Collections, Archives and Recordkeeping (SpARK), and in collaboration with ITDS and departments, schools and administration areas on a programmed basis.

Results of the assessment will be reported to the Information Management Governance Committee.

4.1.5 Compliance and performance monitoring

All aspects of information management require ongoing monitoring, analysis and measurement to ensure that:

- the University's *Information Management Roadmap* is being achieved and policy principles are being met
- benefits are being returned to the University
- required business improvements, efficiencies and digital transformations can be achieved
- risks are mitigated
- insights can be leveraged.

Monitoring of information management practices, processes and systems will be established and coordinated by the University Library, as the business area responsible for the *Information Management Policy*, and in collaboration with ITDS and departments, schools and administrations areas.

The two types of monitoring to be undertaken for information management are compliance monitoring and performance monitoring:

- **Compliance monitoring and compliance auditing** - aim to establish whether a process or procedure is carried out in conformance with relevant external requirements, whether set through legislation, regulations or directions. It involves examining, at a fairly straightforward level, how the University 'does something' and confirming 'compliance' with criteria[iii]
- **Performance monitoring** - involves an in-depth analysis of a process or project, to determine whether it is efficient and effective. It involves developing criteria, conducting interviews and examining documentation to determine how the process or project is conducted. This type of monitoring is also referred to as a process audit[iv].

4.1.6 Quality assurance

Ongoing information management quality assurance is necessary to ensure information is trustworthy and fit for purpose over time.

Quality assurance can require ongoing or targeted assessment of information accuracy, completeness, timeliness, relevance, transparency and consistency.

In accordance with the *Information Management Policy*, Information Custodians, Business System Administrators and the University Library will be responsible for working together to achieve, maintain and report upon quality assurance.

The Information Management Governance Committee will be responsible for receiving regular reports on information management performance and compliance and in turn reporting to the Vice-Chancellor Executive Group as required.

4.1.7 Training

Training and skills development are essential to raise awareness of good information management across the University.

The University has online training modules on recordkeeping and information management available via MyUni, including:

- Recordkeeping induction course
- Electronic Records Management System.

The University Library - Special Collections, Archives and Recordkeeping (SpARK) can also provide tailored training and information sessions to particular business areas and their Personnel on request.

4.2 Plan & design

Information needs to be consciously planned and designed to meet business appropriate requirements and governance needs. To achieve these broad aims, information management planning and design will encompass the following.

- ***information needs assessment*** - assessment of the information that the University needs to design, make and keep and identification of where information requirements need to be built into process, system, service or contract design
- ***information risk assessment*** - identification of where risks to information exist in the University's environments, processes, capabilities or services; identification of policy and compliance risks; implementation of plans to mitigate these risks
- ***information architecture*** - assessment of the architecture needed to support the University's information creation, use, governance and management; alignment of information management needs to enterprise architecture and future conceptual architecture planning
- ***data modelling and design*** - assessment, design and development of the data required to support University operations
- ***information lifecycle planning*** - identification of the requirements and processes needed to support the use and management of information as an asset throughout its lifespan; alignment of systems, services, processes, capabilities and requirements to support information creation, management, use and disposal
- ***information asset registration*** - identification and documentation of core University information assets and systems
- ***evidence and accountability management*** - assessment of University needs for evidence and accountability; planning and assurance exercises to ensure information assets required to support evidence and accountability needs are appropriate, fit for purpose, and kept for as long as required
- ***information system and service management*** - planning and assurance activities to ensure systems and service offerings remain appropriate to University needs; management of the transition of information out of systems and services and into new business appropriate environments when required.[v]

For information management planning and design support and assistance contact the University Library - Special Collections, Archives and Recordkeeping (SpARK). SpARK will collaborate and coordinate efforts with ITDS, Information Custodians, Business System Administrators and the relevant business area/s.

4.2.1 Business systems[vi]

Information management planning and design is particularly important with regards to the selection, development and deployment of business systems across the University.

Business systems are often deployed without an understanding of the business information needs they must support.

Without this understanding, key business information can be at risk. However, information risks can be rectified by clear system planning and governance.

To mitigate risks, system development processes should start with an understanding of:

- what University operations will the system be required to support?
- what information is critical for this business, for Personnel performing the business and for clients?
- what information will be critical into the future for this business, for Personnel performing the business and for clients?
- how long into the future do business and regulatory requirements say this information will be required?
- what information currently supports this business? What additional information would improve business processes?
- what risks to information need to be mitigated in the proposed system?

For further guidance on the management of information assets within business systems, including planning and design, refer to *Standard: Managing digital records in business and records applications* (State Records of South Australia).

The University Library - Special Collections, Archives and Recordkeeping (SpARK), in consultation with the relevant work area of the University and ITDS, is responsible for assessing whether a business system has sufficient information management functionality for capturing and managing University information assets for as long as they are required. To seek an assessment an *Application for Recordkeeping Functionality Assessment* form needs to be completed and submitted by the relevant business area (and in consultation with ITDS as required) to SpARK.

4.3 Create/Receive

4.3.1 When and why to create information assets?

As a general guide, and in order to reflect the University's core functions, Personnel need to create an information asset whenever they do any of the following in connection with the University:

- when making a decision or exercising a University responsibility - it is important to document the fact of a decision and the reasoning behind it; the more significant or weighty the decision, the more thoroughly the reasoning needs to be documented
- when doing something that is important or needs to be accountable - for instance, transactions, contracts, meeting discussions, and things monitored by regulatory agencies
- when taking action that might need to be provided as evidence of in the future - for instance, an action that someone might complain about or challenge
- when doing something that will be useful for any personnel to refer back to in the future - such as something that the University is likely to do again
- as a researcher or teacher, any time something for academic purposes would normally be captured - such as keeping data to substantiate research, recording student grades, or retaining lecture notes for future classes.

Things should be documented as they are happening, or as soon as possible after the event.

Also refer to What is an 'information asset'?

4.4 Organise

4.4.1 Capture

4.4.1.1 When to capture information assets?

Having created an information asset, it needs to be captured in a way that can be found and used in the future. Similarly, when an information asset is received on behalf of the University, such as a letter, email or report, it should also be captured.

As a general guide, information assets need to be captured in all of the following situations:

- when creating any information asset in the course of a University role that could be relevant again in the future - including information assets that would help replicate or re-establish the operations of an area
- when legal or regulatory requirements demand information assets be kept
- when documenting the steps behind a decision, exercise of responsibility or transaction
- when an information asset has been received from or sent outside the University
- when documenting a change to policy, procedure or operational methodology.

Information asset capture needs to be a routine part of each person's University role, and integrated into standard operations and business processes at every level of the institution.

By utilising the University's official recordkeeping system (currently Content Manager TRIM) or University-approved business systems, Personnel ensure that their work is captured and maintained in a managed, secure and well-supported environment that is accessible to them and others as appropriate.

4.4.1.2 What information assets need to be captured?

The University has an obligation to capture anything that shows or explains what is done as an institution, whether created or received. This may include:

- **correspondence** – communications between University Personnel, and between University Personnel and external representatives (eg other Universities, government agencies, students, members of the public, research partners), eg emails and letters
- **core business documents** – documentation of core business processes such as reports, briefing notes, plans, agendas, meeting minutes, working papers, etc
- **financial records** – documentation of financial activity, such as financial reports, budgets, estimates, receipts, contracts, tenders, invoices, statements, etc – the *University's Financial Management Policy* requires that all financial transactions be properly documented and accurately recorded in a timely manner
- **student information** – information assets relating to administering and managing students from application for admission to course or program completion or discontinuation, eg admission, enrolment, academic progress, financial administration and graduation
- **research data and outputs** – information assets of research projects and grants applications, bio-safety, ethical evaluation, animal management, research results and data, commercialisation activities, etc
- **social media** – if an area of the University has a presence on social media, all content and communication (including reactions to posts, comments, tweets, etc) published and transmitted via these platforms are University information assets.

What *doesn't* need to be captured includes:

- **drafts** - generally do not need to keep every draft or old version of a document, unless the older versions actually inform the decision-making process - such as drafts that were distributed to co-workers for comment and came back with remarks that helped guide a decision. Drafts of contracts and other legal documents, which can provide important evidence of a negotiation process, should be retained
- **unimportant/routine administrative documents** – do not need to keep every shred of day-to-day administrative documentation that has only short-term relevance - such as phone messages, rough notes or calculations that lead to more final documents. Common sense should prevail: if a phone message is received from someone who is engaged in a dispute with the University, the message needs to be captured as possible evidence in the dispute; but if a phone message is routine, it is unnecessary
- **copies and published material** – do not need to keep duplicate copies of material, or published materials unless they form an integral part of an information asset.

See also Dispose – Normal Administrative Practice.

4.4.1.3 Where to capture information assets?

Personnel need to ensure information assets and related metadata are captured in University-approved and supported storage. These include:

- the University dedicated electronic recordkeeping system, currently Content Manager TRIM
- business systems institutionally sponsored and supported, such as ResearchMaster, PeopleSoft, Student Administration System, APPoINT, ORBIT, etc,
- institutional-level repositories, for example Aurora.

For more information about storage refer to Store within this section.

4.4.2 Manage metadata[vii]

In order to be authoritative, information assets must possess metadata recording:

- a description of the content of information assets
- the structure of information assets
- the business context in which information assets were created or received and used
- relationships with other information assets and metadata
- business actions and events
- information that may be needed to retrieve and present information assets.

This metadata must be configured in business systems and carried forward through system changes in order to sustain information assets immediately and through time.

This minimum metadata set can be applied to entire systems (such as transactional systems in which all the information assets have the same management requirements) or to individual information assets or groupings of information assets (such as files in an electronic document and records management system (EDRMS), eg Content Manager TRIM).

The metadata described above is the *minimum* required for authoritative information assets. The University may determine the need to create and capture further metadata to ensure that certain information assets are full and accurate and to establish a complete context for them or to prove their authenticity. Such needs will be identified as part of an assessment process conducted by the University Library - Special Collections, Archives & Recordkeeping (SpARK) in consultation with business areas.

Metadata for information assets can also facilitate the management of information assets over time.

The types of metadata which are required to retrieve information assets can also be reused for a range of purposes, including analysis, reporting, service improvement and service monitoring. These additional uses of this type of metadata present opportunities for gaining maximum business value from implementing metadata for information assets.

For further guidance on metadata management refer to *Standard: Minimum Recordkeeping Metadata Requirements* (State Records of South Australia).

4.4.3 Ensure information assets are reliable

Under the *State Records Act 1997* the University is forbidden from altering or interfering with records once they have been created and captured - and is only allowed to destroy records in accordance with specific disposal rules and schedules.

If Personnel discover a problem or error with an information asset they have already captured into a University business system, they are not permitted to change or destroy it. Instead, create a new information asset related to the previous one, and if appropriate, add a note explaining why the old version should not be used, and store these together.

For information assets captured into Content Manager TRIM, Personnel can use revisions to keep track of changes and finalise the last revision.

As a general guide, the following techniques will help ensure reliability of information assets:

- use revisions to trace the development of an information asset
- save final, signed documents in PDF format (or as "Finalised" if in Content Manager TRIM) so that they cannot be edited - and so that it is clear later on which version was ultimately distributed.

By applying such techniques, Personnel help ensure that any information asset created or received is (and remains) reliable evidence of University activity.

4.4.4 Ensure information assets are findable

There are various reasons why information assets need to be found over time:

- they may be requested under freedom of information
- they may be requested through a warrant or subpoena
- they may be needed to meet reporting requirements internally or externally
- they may be needed to explain and/or justify a past decision
- Personnel may want to learn from a past situation or action.

Not only do information assets need to be findable on demand they should be able to be located with minimal effort.

By using the University's official recordkeeping system, Content Manager TRIM, the ability to easily find information assets is assured - Personnel can search for an information asset and either view an electronic copy if it is available in the system, or determine where the relevant asset is physically located.

If other business systems are used to store information assets, such systems need to have adequate information management functionality or be integrated with Content Manager TRIM. It is the responsibility of Business System Administrators to ensure this on behalf of business areas and Personnel.

4.4.5 Store

4.4.5.1 Storing active information assets

It is important to keep information assets being used for current business needs in conditions that ensure they are protected, secure and accessible for as long as they are required to meet the business requirements and legal obligations of the University.

Regardless of whether information assets are hardcopy or digital, the following are recommended to ensure effective storage:

- store information assets in a way that will protect them from unauthorised access or disclosure, especially assets that are sensitive
- information assets that originate in a digital form should remain digital
- hardcopy files that are registered in Content Manager TRIM can be returned to the University Library - Special Collections, Archives & Recordkeeping (SpARK) when they are no longer required by Personnel
- determine what information assets need to be stored in a work area for immediate access and useability versus more remote storage. If hardcopy records need to be consulted frequently, keep them within office space
- use the University's disposal schedules to help prioritise information assets for storage. For instance, if information assets are only required to be stored for a short period of time (such as less than 2 years) then it may be more efficient to keep them on site until they can be destroyed. By contrast, information assets identified for permanent retention will require the highest standards of care to ensure their longevity
- vital records need to be stored in Content Manager TRIM. Hard drives and personal email folders are not accessible to other Personnel and records can be lost when Personnel leave the University

- standard email programs and shared network drives *do not* provide information management functionality such as adequate metadata, access and security. These, therefore, are not suitable to meet the University's obligations under the State Records Act.

For assistance in evaluating storage options for active information assets consult with the University Library - Special Collections, Archives & Recordkeeping (SpARK).

4.4.5.2 Long-term storage

Some information assets that are no longer required for current business purposes still need to be stored and retained for further periods or indefinitely as archives in accordance with disposal schedules (refer to Dispose – disposal schedules for further information) and/or compliance obligations (refer to Compliance requirements relating to information management for further information).

When information assets are no longer required for active use contact the University Library - Special Collections, Archives and Recordkeeping for an assessment of information assets and/or the business systems in which they are held. Advice will then be provided regarding the need to:

- maintain the existing business system and its information assets until they can be legally destroyed OR
- migrate the information assets to a different system to ensure their storage and retention until they can be legally destroyed OR
- transfer or migrate the information assets to the University Archives for longer-term or permanent (in the case of archives) storage.

4.5 Use & Re-Use

4.5.1 Manage access – the basics

The following basic principles enable access to information assets to be managed in the most balanced and appropriate way:

- only restrict access where there is a good reason - such as privacy, commercial confidence, legal privilege or intellectual property protection - and only restrict those portions of an information asset that truly need to be restricted
- only restrict access for as long as the restriction is properly required
- if something is confidential, ensure the information asset says so (either directly or in metadata) and explains why in a way that any Personnel looking at the information asset would understand
- adhere to the rules surrounding privacy, especially Personnel working with student or staff records
- throughout the life of an information asset, regularly review whether if it still needs to have its access restricted
- create and use digital information assets where possible, to improve findability and the proper management of access
- if access is sought to any University information assets by someone from outside through Freedom of Information, the request must be escalated promptly to the

University's FOI officer who assist in processing the application within the strict time limits prescribed by the law

- if access is sought by a warrant/subpoena, the request needs to be dealt with promptly, as the request may have time limitations that are legally binding. For areas with clear procedures for dealing with such requests (such as student records), follow those procedures carefully and seek further advice if necessary. For areas that have no such internal procedures, seek assistance from Legal and Risk Branch
- if it is unclear whether access should be granted to a particular information asset, seek advice from the University Library - Special Collections, Archives & Recordkeeping (SpARK).

4.5.2 Privacy, confidentiality and other limits on access

It is best practice *not* to restrict records in order to facilitate sharing of knowledge. However, in some instances there is a demonstrated need to restrict access, including:

- **personal information** - many of the information assets held by the University contain personal information, eg student records, personnel files. Any information or opinion from which the identity of an individual can be ascertained is considered to be "personal information". For further details, refer to the *Privacy Policy and Management Plan*
- **financial information** – eg tax file numbers, bank account or credit card details. These are a form of personal information, but are also generally subject to specific confidentiality requirements under financial regulations. For more information, consult with Financial Services or someone in Legal and Risk Branch
- **health-related information** - eg counselling notes or medical information. In addition to being a form of sensitive, personal information, they are subject to additional regulatory and professional confidentiality requirements
- **student-related information** - eg grades, progress and enrolment details of current, past and prospective students (including those who are offered a place but ultimately do not attend the University)
- **legally-privileged documents** - eg communications between Personnel and legal representatives (including the Legal and Risk Branch of the University) or advice received from legal representatives. For further information, ask the Legal and Risk Branch
- **information requiring confidentiality to ensure intellectual property right protection** - eg patentable information which is in the course of being protected. For more information, contact Innovation and Commercial Partnerships
- **commercially-sensitive information** - eg information provided by an industry sponsor in the course of a specific research project, disclosed on the basis of "commercial in confidence". Commonly this material would be protected by way of a confidentiality agreement (or confidentiality clauses in the research funding contract)
- **confidential by way of agreement** - if the University has agreed to keep something confidential under a contract, then it must comply with that agreement. If agreeing to keep something confidential, run the terms by a legal advisor, such as someone in Legal and Risk Branch. Note that if the terms of a contract itself are intended to be kept confidential, then a special process must be followed before the contract is signed, otherwise the document will not be protected from access under Freedom of Information. For more details, refer to the *Freedom of Information Policy*.

4.5.3 Information classification[viii]

Implementing consistent methods of classification allows sensitive information to be securely shared with confidence that the information will be handled and protected according to its sensitivity.

In relation to security, there are generally two types of information asset held by the University:

- information that does not need increased security
- information that needs increased security to protect its confidentiality.

Most information assets do not need increased security and may be marked as unclassified or left unmarked. This should be the default position for newly-created information assets, unless there is a specific need to protect the confidentiality of the information.

An information asset only requires increased security to protect its confidentiality if its compromise could damage University interest, organisations or individuals or requires protection under legislation or contractual requirements.

An information asset which needs increased protection is to be security classified in accordance with the ITDS *Security Classification guidelines*.

Over-classification is to be avoided as it has a range of undesirable outcomes, including:

- unnecessary limitation of public access to information
- unnecessary imposition of extra administrative arrangements and additional cost
- excessively large volumes of protected information, which is harder for the University to protect
- devaluing protective markings so that they are ignored or avoided by Personnel or receiving agencies.

4.5.4 Security[ix]

Security is ‘the preservation of the confidentiality, integrity and availability of information':

- **confidentiality** - ensuring that information is accessible only to those authorised to have access
- **integrity** - safeguarding the accuracy, completeness and authenticity of information and processing methods
- **availability** - ensuring that authorised users have access to information assets when required.

Information security applies to all forms of information (digital, paper-based or other) and includes the management of the software and/or communications technology systems and networks for storing, processing, communicating and disposal of information.

In implementing adequate security measures, the University is responsible for assessing its information assets, irrespective of format, and:

- identifying vital information assets and systems
- identifying high risk and high value information assets and systems
- identifying the level of protection needed based on sensitivity, confidentiality and value

- assigning roles and responsibilities for the management of vital, high value and high risk information assets and
- putting in place controls according to their classification and relevant compliance requirements.

The *Australian Standard AS/NZS ISO/IEC 27002:2006 Information technology – Security techniques – Code of practice for information security management* establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation. It contains best practice guidance concerning a number of areas of information security management.

Refer to the section on *using information assets remotely* for guidance on ensuring security where information assets are being portably used.

If a restricted or confidential information asset is subject to unauthorised access, unintentional disclosure, or has its security breached in any other way (including through loss or misplacement of the information asset), act in accordance with the University's *Data Breach Response Plan*.

4.5.5 Cyber security[x]

Cyber security covers the controls the University must put in place to protect information stored in networks and systems. It includes responding to evolving threats such as viruses/malware, hacktivism or phishing attempts.

Effective cyber security includes:

- implementing cyber security planning and governance
- building and supporting a cyber security culture across the University
- managing cyber security risks to safeguard and secure University information assets and systems
- improving resilience, including the University's ability to rapidly detect cyber incidents, and respond appropriately
- reporting against the University's cyber security requirements and measures.

For further information refer to the *IT Acceptable Use and Security Policy* and the ITDS Secure IT webpage.

ITDS also provides an online cybersecurity tutorial, which all Personnel are required to complete.

4.5.6 Public Access

4.5.6.1 Freedom of Information (FOI)

The *Freedom of Information Act 1991* is a state law that gives members of the public a right to access the University's information assets - with some exceptions, such as where information assets contain personal or confidential information, or are subject to some other reasonable limitation (such as being legally privileged, or commercially sensitive).

If an FOI request is received by Personnel or local area, contact the University's FOI Officer immediately. They will coordinate the University's response, and help determine which documents (if any) may be subject to exemptions from disclosure under the legislation.

For additional information, refer to the Freedom of Information (FOI) section of the University website and the *Freedom of Information Policy*.

4.5.7 Research Data

4.5.7.1 Open Access

The University supports the open access release of scholarly works and research outputs.

For further information refer to the *Open Access Policy* or contact the Copyright and Open Access Coordinator.

4.5.7.2 FAIR Data Principles[xi]

The University endorses the FAIR (Findable, Accessible, Interoperable, Reusable) Data Principles and their application to data (or any digital object), metadata (information about that digital object), and infrastructure (eg a searchable resource) in order to optimise re-use of research outputs.

4.5.8 Remote use of information assets

Portability of information assets is a reality that is recognised by the University. However, Personnel are required to take certain steps to ensure the proper management of any being used remotely:

- when creating either electronic or hardcopy University information assets away from the office they still need to be captured into a University-approved and supported system either by remote means or the next time Personnel is back on site
- ensure the security of information assets and report any loss or unauthorised access to a Head of School or Branch (who should be made aware if information assets have been compromised in accordance with the University's *Data Breach Response Plan*), to the ITDS Helpdesk for electronic information breaches (refer to *IT Security Procedures*), and to the Legal and Risk Branch (who must be informed for insurance purposes, and who may be able to provide assistance dealing with the situation)
- never remove the only copy of an information asset from the University - for hard copy assets, leave the original on campus and take a copy to work from
- use password protection or a locked briefcase to prevent unauthorised access to information assets that are being used off-site
- to ensure that emails are preserved on a University system, either use webmail when working remotely or configure remote email applications so that University email is never downloaded remotely without also leaving a copy on the University server.

4.5.9 Business intelligence and analytics[xii]

Business intelligence and analytics refers to the technologies, systems, practices, and applications that analyse critical business data to help an enterprise better understand its business and market and improve decision making.

Business intelligence and analytics encompasses:

- **data analytics** - activities involving the definition, collection and assessment of data to develop insights, strategic directions and business improvements
- **business intelligence** - processes for analysing information to optimise University decisions and performance

- **big data, streaming data and internet of things** - design, management, storage and utilisation of the data generated from the network of devices and sensors that connect and exchange data, to generate University efficiencies and intelligence
- **artificial intelligence, machine learning and predictive analytics** - design, management and implementation of processes to enable machines to learn from experience, through processing large amounts of data and recognising patterns in the data, to automate activities or to make predictions about the future
- **geospatial and location intelligenc**e - design, management and implementation of processes to use location information to derive meaningful University insights that improve service delivery and planning
- **reporting and insight management** - processes for ensuring that the insights generated through business intelligence and analytics activities are retained, applied and fed back into University and quality improvement activities.

The University's business intelligence and analytics is dependent on its ability to re-use information assets that are accurate, reliable, findable and well-managed.

For further information about the University's business intelligence and analytics contact Planning & Analytics.

4.6 Dispose

4.6.1 Disposal schedules

The *State Records Act 1997* requires information assets to be disposed of in accordance with approved Disposal Schedules, which set out the legally mandated minimum retention periods and disposal actions for various kinds of information assets.

For the University the following disposal schedules specifically apply:

- *General Disposal Schedule 24 for Universities of South Australia* (GDS 24)
- *General Disposal Schedule 30 for Administrative Records* (GDS30).

In accordance with the disposal schedules, some information assets are of temporary value only and can be destroyed after defined periods of time. Such retention periods can range from 1 year to 100+ years, depending on the functions and activities that are documented.

Other information assets are deemed to be of permanent value, either due to requirements of the disposal schedules or due to the fact that they have an enduring value to the University.

4.6.2 Disposal in the digital environment[xiii]

Much of University operations today is performed within digital systems, applications and services. It is therefore vital that information retention and disposal rules are considered at:

- system design
- system procurement
- system implementation
- transitions to cloud services
- contract negotiations for cloud services
- portability planning for cloud services

- business process outsourcing
- application development.

As a risk management approach, the University will:

- prioritise actions, focussing on high risk/high value business systems and medium to long term information retention requirements (where information assets are required for 5+ years)
- specifically identify and assess business systems containing information assets that need to be retained 10+ years and determine continuity strategies to ensure these information assets can be accessed, trusted and used for as long as they are legally required to be kept.

The University Library - Special Collections, Archives & Recordkeeping (SpARK), ITDS and business areas will work together to ensure the above. In implementing information asset disposal 'by design' the following risks to the University are mitigated:

- increased and unsustainable storage costs
- increased and unsustainable management costs
- loss of high value information assets in amongst the 'noise'
- increased risk of inadvertent data loss through large-scale data purging
- increased costs through a 'keep everything' approach
- poorly-managed and costly services.

4.6.3 Making disposal decisions

Disposal actions will be applied automatically to information assets if they have been previously captured into:

- the University dedicated electronic recordkeeping system, currently Content Manager TRIM
- business systems institutionally sponsored and supported, such as ResearchMaster, PeopleSoft, Student Administration System, APPoINT, ORBIT, etc – these systems either have adequate information management functionality or have been integrated with Content Manager TRIM (see also *Business Systems*)
- institutional-level repositories, for example Aurora.

If information assets are under local area custody and have *not* been captured into Content Manager TRIM or business systems institutionally sponsored and supported then the relevant business area must contact the University Library – Special Collections, Archives and Recordkeeping (SpARK) for a disposal authorisation request to determine what information assets are temporary and what may be permanent. This form will be returned with instructions on the appropriate retention period and disposal action.

4.6.4 Destruction of temporary value information assets

The destruction of University information assets, with the exception of NAP material (refer to the section *Normal Administrative Practice (NAP)*) must be authorised by the University Library - University Archivist, in accordance with the *Information Management Policy*.

For information assets captured in Content Manager TRIM, the University Library – Special Collections, Archives and Recordkeeping (SpARK) monitors when destruction of temporary records is due and consults with business owners of the information assets before any disposal occurs.

For information assets captured in business systems or kept in local area custody, the relevant business area must contact and seek written approval from the University Library - University Archivist before any destruction takes place.

4.6.5 Normal Administrative Practice (NAP)[xiv]

NAP is the concept that material can be destroyed according to 'normal administrative practices'. This provides for the routine destruction of drafts, duplicates and publications, with the test that it is obvious that no information of continuing value to the University will be destroyed. Destruction under NAP does *not* require the authorisation of the University Archivist.

Material that can be disposed of under NAP comprises items of an ephemeral or transitory nature created, acquired or collected by Personnel in the course of their official duties. Such material has no ongoing value and is not usually incorporated into the official recordkeeping system or business systems.

NAP falls into six main groups:

- transitory or short term items, eg phone messages, notes, compliment slips, office notices and circulars
- rough working papers and/or calculations created in the preparation of information assets
- drafts not intended for further use or reference, excluding official version drafts of agreements, submissions and legal documents
- duplicate copies of material retained for reference purposes only
- published material which does not form an integral part of an information asset
- system printouts used to verify or monitor data, or answer ad-hoc queries that are not part of regular reporting procedures and not required for ongoing use.

4.6.5.1 The NAP test

Where material is *not* duplicated in the official recordkeeping system or business systems, Personnel need to consider:

- does the material form part of a University transaction?
- does it add value to an existing information asset?
- does it show how a transaction was dealt with?
- does it show how a decision was made?
- does it show when or where an event happened?
- does it indicate who was involved or what advice was given?
- is it a formal draft of a Cabinet submission, an agreement or a legal document?
- is the material included in a disposal class in a general disposal schedule or in an agency operational disposal schedule?

If the answer to any of these questions above is ***YES*** then the material must not be destroyed according to NAP.

Therefore, the following types of items may be destroyed under NAP:

- word-processing documents and spreadsheets in electronic format after updating, printing, or transfer to official recordkeeping system or business systems
- drafts and rough notes not intended for further use
- brochures, catalogues, price lists, unsolicited promotional material etc received from external sources
- superseded copies of instructions, guidelines, standards, etc not included in a general or agency records disposal schedule
- extra copies of information assets no longer required for reference purposes
- copies of published items kept for personal reference
- unimportant messages and notes, eg those required for only few hours or a few days
- system printouts used to verify or monitor data, or answer ad-hoc queries that are not part of regular reporting procedures and are not required for ongoing use.

NAP is provided in the interest of efficient information management and extends to material of ephemeral and transitory value *only*.

4.6.6 Information assets required for legal purposes, inquiries and/or investigations[xv]

Information assets cannot be destroyed if they are likely to be required for legal purposes. If an investigation, inquest, commission or inquiry is in progress (or forecast in Parliament or the press) all relevant information assets need to be identified and retained until the action, and any subsequent actions, are completed or appeal periods have lapsed.

Seek advice from the Legal and Risk Branch if there is any possibility that destruction of an information asset could be prejudicial to the interests of the University, its Personnel, students, partners or other stakeholders.

4.6.7 Decommissioning of business systems and websites

4.6.7.1 Business systems[xvi]

Decommissioning is a process by which a business application (or system) is removed from use in the University. Decommissioning requires:

- analysis of the information assets in the system
- identifying the information assets, associated metadata and system documentation that must be brought forward and retained and
- an accountable process for deletion of residual information assets in the system no longer required.

A business system needs to be decommissioned when either:

- the system is replaced by a new target system covering the same functionality or
- the system is obsolete because it no longer supports a business process of the University.

All business systems will eventually become legacy systems due to rapidly changing technology and business environments.

Common scenarios in which decommissioning occurs include:

- new system implementation projects that involve consolidating and rationalising multiple legacy systems
- applications/systems which no longer support core University processes due to implementation of new systems
- infrastructure rationalisation projects to reduce maintenance and storage costs.

Protecting information assets is a core responsibility of the University during a decommissioning project, and will often require migration of information assets to a new business system. However, decommissioning also provides an opportunity to legally dispose of information assets which are no longer required.

Before a business system is decommissioned, ITDS and the relevant business area/s need to liaise with the University Library- Special Collections, Archives and Recordkeeping (SpARK) with regards to both the migration of information assets to a new system and the destruction of any information assets within the existing system. An *Authorisation for the Disposal of Official Records in an Approved University Business System* form will need to be completed. The University Archivist is then responsible for approving the migration and disposal of information assets.

4.6.7.2 Websites

Websites are considered information assets for the purposes of the University's *Information Management Policy*.

Some of the University's websites will be of enduring value and will therefore need to be retained and made accessible as archives.

The University Library - Special Collections, Archives and Recordkeeping (SpARK), is responsible for the University's web archiving tool and related services. Contact SpARK for further advice and assistance prior to the decommissioning of University websites.

4.6.8 Archives

The University Library is responsible for the University's archives program that ensures the ongoing care and preservation of University information assets of enduring value and significance, ie those considered to be worthy of permanent retention.

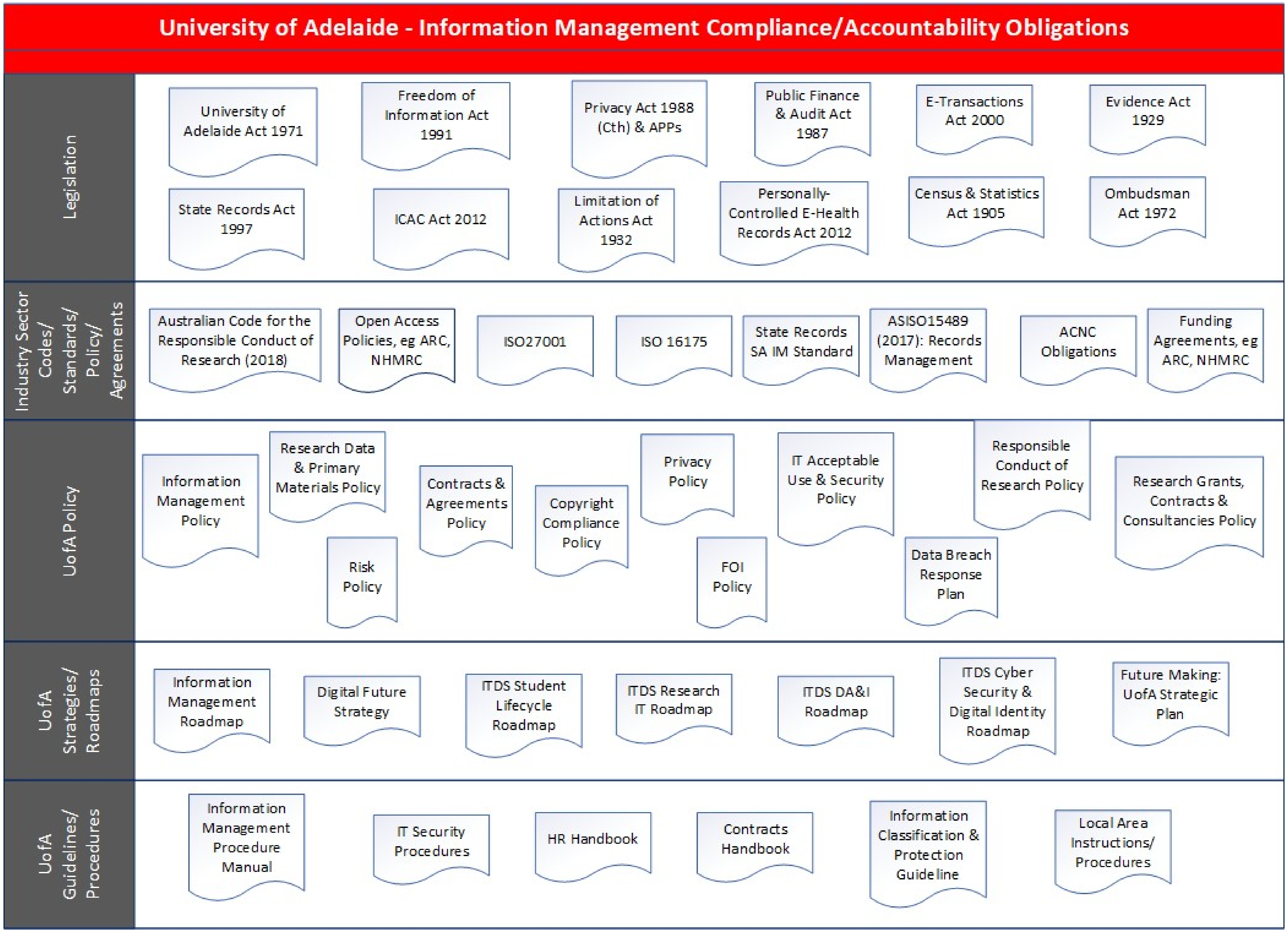
Information assets which are retained permanently include:

- information assets with **administrative value**, eg minutes and agendas of senior committees, policies and procedures, annual reports, campus maps and other records retained to meet the continuing administrative needs of the University
- information assets with **legal value**, eg agreements, certificates of title, delegations of authority and other documents that must be preserved in order to protect the legal rights of the University, its Personnel and its students
- information assets with **financial value**, eg high level financial statements, returns and audit reports that demonstrate the conduct of the University's financial affairs in a transparent and honest manner

- information assets with **informational value** (or community value), eg records that add context and texture to the history of the University, or demonstrate social, political and recreational aspects of the University community and its position within South Australia and beyond. Photographs, media releases and promotional material may fall under this category, as well as records related to any events or controversies in the University community that are historically interesting.

For advice and assistance on how and where your permanent information assets should be archived, contact the University Library - Special Collections, Archives and Recordkeeping (SpARK).

Attachment 1: IM Compliance



University of Adelaide - Information Management Compliance/Accountability Obligations

Legislation

- University of Adelaide Act 1971
- Freedom of Information Act 1991
- Privacy Act 1988 (Cth) & APPs
- Public Finance & Audit Act 1987
- E-Transactions Act 2000
- Evidence Act 1929
- State Records Act 1997
- ICAC Act 2012
- Limitation of Actions Act 1932
- Personally-Controlled E-Health Records Act 2012
- Census & Statistics Act 1905
- Ombudsman Act 1972

Industry Sector Codes/ Standards/ Policy/ Agreements

- Australian Code for the Responsible Conduct of Research (2018)
- Open Access Policies, eg ARC, NHMRC
- ISO27001
- ISO 16175
- State Records SA IM Standard
- ASISO15489 (2017): Records Management
- ACNC Obligations
- Funding Agreements, eg ARC, NHMRC

UofA Policy

- Information Management Policy
- Research Data & Primary Materials Policy
- Risk Policy
- Contracts & Agreements Policy
- Copyright Compliance Policy
- Privacy Policy
- FOI Policy
- IT Acceptable Use & Security Policy
- Data Breach Response Plan
- Responsible Conduct of Research Policy
- Research Grants, Contracts & Consultancies Policy

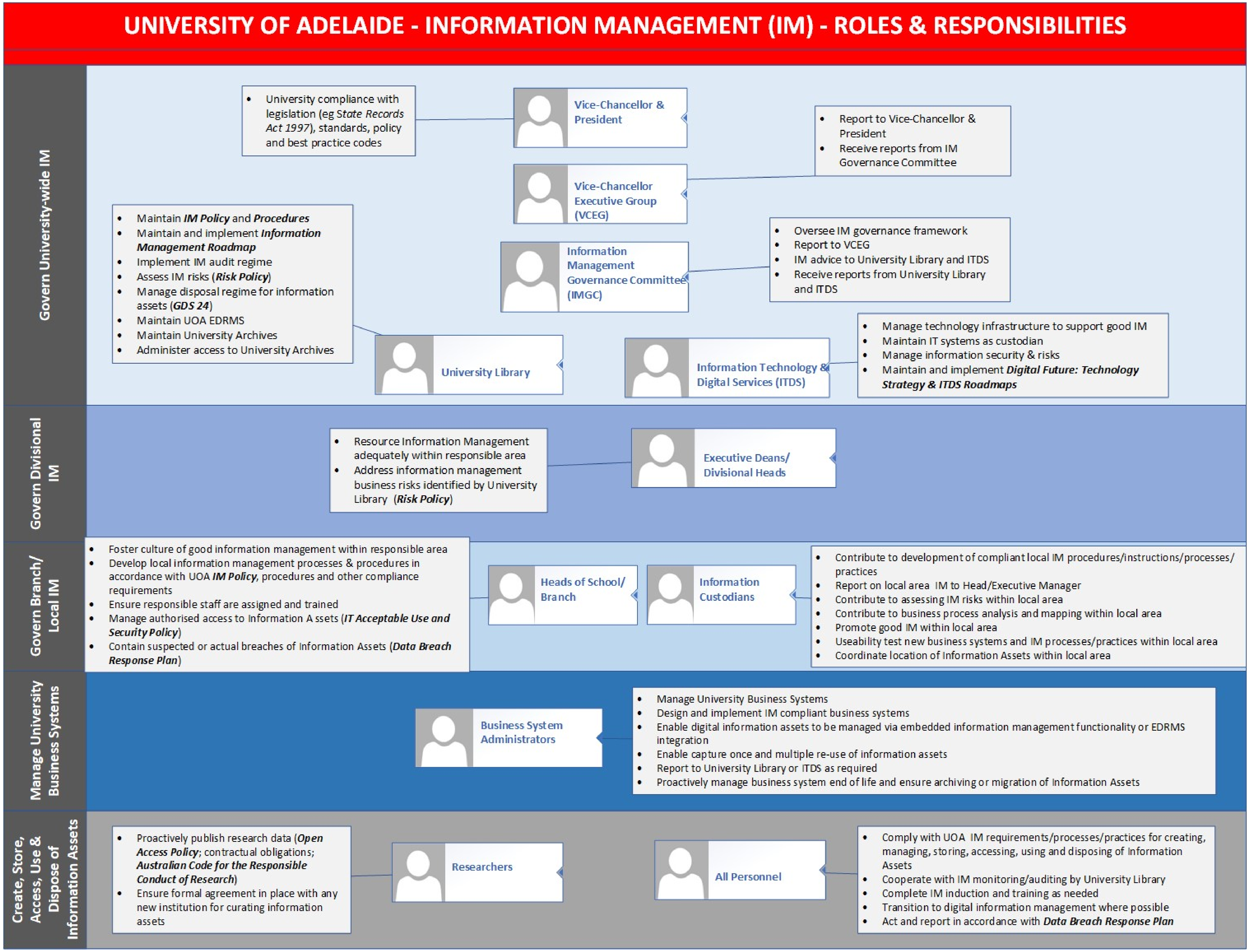
UofA Strategies/ Roadmaps

- Information Management Roadmap
- Digital Future Strategy
- ITDS Student Lifecycle Roadmap
- ITDS Research IT Roadmap
- ITDS DA&I Roadmap
- ITDS Cyber Security & Digital Identity Roadmap
- Future Making: UofA Strategic Plan

UofA Guidelines/ Procedures

- Information Management Procedure Manual
- IT Security Procedures
- HR Handbook
- Contracts Handbook
- Information Classification & Protection Guideline
- Local Area Instructions/ Procedures

Attachment 2: IM Roles & Responsibilities



UNIVERSITY OF ADELAIDE - INFORMATION MANAGEMENT (IM) - ROLES & RESPONSIBILITIES

Govern University-wide IM

Vice-Chancellor & President

- University compliance with legislation (eg *State Records Act 1997*), standards, policy and best practice codes

Vice-Chancellor Executive Group (VCEG)

- Report to Vice-Chancellor & President
- Receive reports from IM Governance Committee

Information Management Governance Committee (IMGC)

- Oversee IM governance framework
- Report to VCEG
- IM advice to University Library and ITDS
- Receive reports from University Library and ITDS

University Library

- Maintain ***IM Policy*** and ***Procedures***
- Maintain and implement ***Information Management Roadmap***
- Implement IM audit regime
- Assess IM risks (***Risk Policy***)
- Manage disposal regime for information assets (***GDS 24***)
- Maintain UOA EDRMS
- Maintain University Archives
- Administer access to University Archives

Information Technology & Digital Services (ITDS)

- Manage technology infrastructure to support good IM
- Maintain IT systems as custodian
- Manage information security & risks
- Maintain and implement ***Digital Future: Technology Strategy & ITDS Roadmaps***

Govern Divisional IM

Executive Deans/ Divisional Heads

- Resource Information Management adequately within responsible area
- Address information management business risks identified by University Library (***Risk Policy***)

Govern Branch/ Local IM

Heads of School/ Branch

- Foster culture of good information management within responsible area
- Develop local information management processes & procedures in accordance with UOA ***IM Policy***, procedures and other compliance requirements
- Ensure responsible staff are assigned and trained
- Manage authorised access to Information Assets (***IT Acceptable Use and Security Policy***)
- Contain suspected or actual breaches of Information Assets (***Data Breach Response Plan***)

Information Custodians

- Contribute to development of compliant local IM procedures/instructions/processes/ practices
- Report on local area IM to Head/Executive Manager
- Contribute to assessing IM risks within local area
- Contribute to business process analysis and mapping within local area
- Promote good IM within local area
- Useability test new business systems and IM processes/practices within local area
- Coordinate location of Information Assets within local area

Manage University Business Systems

Business System Administrators

- Manage University Business Systems
- Design and implement IM compliant business systems
- Enable digital information assets to be managed via embedded information management functionality or EDRMS integration
- Enable capture once and multiple re-use of information assets
- Report to University Library or ITDS as required
- Proactively manage business system end of life and ensure archiving or migration of Information Assets

Create, Store, Access, Use & Dispose of Information Assets

Researchers

- Proactively publish research data (***Open Access Policy***; contractual obligations; ***Australian Code for the Responsible Conduct of Research***)
- Ensure formal agreement in place with any new institution for curating information assets

All Personnel

- Comply with UOA IM requirements/processes/practices for creating, managing, storing, accessing, using and disposing of Information Assets
- Cooperate with IM monitoring/auditing by University Library
- Complete IM induction and training as needed
- Transition to digital information management where possible
- Act and report in accordance with ***Data Breach Response Plan***

[i] For definition of Personnel as relevant to information management refer to the *Information Management Policy*.

[ii] Adapted from *Information Management Framework*. 2018. Digital.NSW, p.9.

[iii] CB029 - 2003, *The Audit Skills Handbook*, section 1.8

[iv] ibid

[v] Adapted from *Information Management Framework*. Op cit. p.11.

[vi] Adapted from *Developing Systems: information management considerations*. State Archives and Records Authority (SARA) NSW. April 2014. https://www.records.nsw.gov.au/recordkeeping/advice/developing-systems-considerations . Accessed 10 July 2020.

[vii] Adapted from Minimum requirements for metadata for authoritative records and information. State Archives and Records Authority (SARA) NSW. Updated June 2019. https://www.records.nsw.gov.au/recordkeeping/advice/metadata-for-records-and-information/minimum-requirements . Accessed 10 July 2020.

[viii] Adapted from *Information Classification, Labelling and Handling guidelines. Digital.NSW.* July 2015.

[ix] Adapted from Information Securityh FAQs. State Archives and Records Authority (SARA) NSW. February 2019. https://www.records.nsw.gov.au/recordkeeping/advice/information-security . Accessed 10 July 2020.

[x] Adapted from *Cyber Security Policy*. Digital.NSW. February 2019.

[xi] Further information on the FAIR Data Principles is available, eg from the Australian Research Data Commons https://ardc.edu.au/resources/working-with-data/fair-data/ .

[xii] Adapted from *Information Management Framework*. Op cit. p.14.

[xiii] Adapted from State Archives and Records Authority (SARA) NSW. Accessed 10 July 2020.

[xiv] *General Disposal Schedule 30 for Administrative Records*. Version 2. State Records of South Australia.

[xv].ibid.

[xvi] Adapted from *Decommissioning systems: records and information management considerations*. State Archives and Records Authority (SARA) NSW. April 2018. https://www.records.nsw.gov.au/recordkeeping/advice/decommissioning-systems . Accessed 10 July 2020.