Information Management Framework

DOCUMENT MANAGEMENT

Version *<v.YYYY.0x>*	v.2025.01
Release *<Draft or Current>*	**CURRENT**
Release Date *<dd/mm/yyyy>*	17/03/2025
Next Review Date *<dd/mm/yyyy>*	01/07/2025
Authorised By:	Director Information and Records Management, Siddhant
Document Managed By:	Records Manager, Catherine Nicholls & Senior Records Analyst, Karyn Lemon
Comments and Questions:	groupinformationmanagement@monash.edu

Table of Contents

Purpose

Monash University's information is a valued asset that underpins effective and efficient operations, provides transparency and accountability as well being required for legal, evidentiary and historical purposes. Data and information continues to play a growing role in shaping Monash's strategic direction. Records of Monash's decisions and actions are also an essential source of information for effective and responsive management. As our reliance on data, information and records increases, it is essential that these resources are managed appropriately throughout their required lifespan.

To achieve this, clear and effective information governance structures and practices must be implemented. The Information Governance and Management Framework provides a consistent approach to information governance and management at Monash University.

This document defines our information governance and management roles, authorities, and structures to:

- support Monash's strategic objectives;
- ensure Monash protects and preserves its information in line with relevant University policies and procedures including Data Privacy and Protection, Cyber Security and Risk Management;
- enable effective, ethical, and secure use of data, information, and records;
- meet legislative and administrative obligations in particular those relating to the management of public records, data protection and privacy, as well as Freedom of Information.

This framework both supports and provides practical steps towards implementing the principles outlined in both the Monash University's Information Management Policy and Information Governance and Recordkeeping Procedure.

Scope

For the purpose of this framework references to 'Monash' include Monash University Australia, Monash University Malaysia, Monash University Indonesia, Monash Suzhou, the Monash University Prato Centre, and the World Mosquito Program Ltd (and its subsidiaries).

In Scope

This framework applies to all Monash University staff, students, associates and visitors who handle information (records, information, and data) in any format, including Research Administration activities.

Out of Scope

Information (records, information, and data) that directly relate to Research data management is outside the scope of this Information Management Governance Framework. See Research Data at Monash for more information.

Legislative Obligations

The University has a legal obligation to manage its records properly. All records at Monash, including paper documents, electronic files, photographs, maps, films, sound recordings, and emails, are considered public records.

Digital Monash records are stored in various IT systems, software and platforms which can include locally managed documents and emails, social media accounts, as well as team and collaborative environments. Records can exist on different platforms and be stored on local servers or in the cloud.

All records created by Monash are considered public records.Therefore, Monash must ensure that all of its data management, information management and recordkeeping processes and practices are in alignment with relevant legislative requirements including:

- Public Records Act (Vic) 1973
- Information Privacy Act (Vic) 2000
- Health Records Act (Vic) 2001
- Privacy Act (Cth) (1988)
- Copyright Act (Cth) 1968
- Electronic Transactions Act (Vic) 2000
- Higher Education Support Act (Cth) 2003
- Evidence Act (Vic) 1958
- Public Interest Disclosures Act 2012 (Vic) 2012
- Freedom of Information Act (Vic) 1982
- Crimes Act (Vic) 1958 *(in particular, provisions relating to document falsification, destruction and suppression etc)*
- General Data Protection Regulation (GDPR) (EU) 2018

This is not an exhaustive list of all the possible legislative acts that impact on recordkeeping. These particular examples also relate specifically to Victorian campuses and may not apply in the same way to records created on Monash's overseas campuses. *It should be noted that the Information Management Policy (that this Framework supports), operates in jurisdictions outside of Australia to the extent permitted by both the law and related government policy of those jurisdictions. In relation to Monash University campuses or other operations outside of Australia; a reference below to 'law' is a reference to the law governing that campus or those operations. Where local legislation is silent or prescribes a lesser requirement, Monash will adopt the higher standards to ensure compliance and uphold its commitment to best practices in information management.* For questions about recordkeeping and specific legislative acts and Monash's overseas campuses please contact Group Information and Records Management for advice.

Monash must ensure that it also complies with relevant external government recordkeeping standards including:

- Public Record Office Victoria Standards

It is also important that all internal procedures that relate to data, information and recordkeeping are adhered to including:

- Freedom of Information
- Data Protection and Privacy
- Cyber Security Policy and Standards
- University Retention and Disposal Authority

Information Governance

Monash recognises that data, information and records exists at both a local level, e.g.

- an individual staff member's email account and/or team collaborative level, e.g.
- shared and collaborative spaces such as G-Suite files or File Share.

Data, information and records are also managed in Monash information assets, e.g.

- hardcopy and digital repositories managed by University Archives and the University Library.
- data, information and records held within University IT systems, software and platforms (such as Callista, SAP, TRIM, UniCRM, PURE, etc).

While the principles outlined in the University's Information Management Policy and accompanying procedures apply regardless of where University data, information and records exist, there are different layers of responsibility that apply to different roles within the organisation.

Roles and Responsibilities

Monash University as an entity

Monash University is the responsible custodian of all of its data, information and records.

Monash is subject to a wide range of regulatory compliance obligations, including compliance requirements under applicable laws, regulations, and industry standards. Monash adopts a risk-based approach to managing regulatory compliance obligations by maintaining controls that seek to ensure that it upholds those obligations (typically an operational process that gives effect to an obligation).

Vice Chancellor and President

In accordance with PROS 23/01 Strategic Management Standard, the University Vice-Chancellor and President is accountable and responsible for organisational compliance with the Public Record Office Standards established under the Public Records Act (Vic) 1973. The head of the public office (i.e. the University) is responsible for authorising strategies and policies and implementing a monitoring regime which measures compliance with the Standards and reports to PROV as required.

Information Creators

All staff, students and associates are responsible for being ethical, transparent, proactive, accountable and cooperative in creating and managing Monash data, information and records. As such, within the context of this framework, all staff, students and associates will be referred to as Information Creators.

An Information Creator is responsible for:

- accurately and ethically creating and capturing information and data in both local & team environments (e.g. G-Suite, file shares) and University information assets (e.g. IT systems, software and platforms);
- ensuring the appropriate information security classification is assigned (in accordance with direction from Information Stewards) when information is created or captured into University information assets;
- complying with relevant legislation as well as Monash-wide and business area specific policies, procedures, and controls; and
- seeking advice from Group Information and Records Management as required.

Information Consumers

Information Consumers use the Monash data, records and information that they have been granted access to, for authorised purposes only. As such, Information Consumers include University Information Creators, as well as other nominated, authorised/approved external entities or individuals who wish to access data, information or records held within the custody of Monash.

Information Consumers are responsible for:

- using the University's data, records and information in compliance with all relevant legislation as well as Monash-wide and business area specific policies, procedures and controls;
- using the University's information ethically and securely while respecting confidentiality and privacy;
- ensuring the information they consume is fit for its specific purpose/s; and
- providing feedback about the quality of information to relevant Monash representatives.

Within in the context of managing University information assets, including Monash IT systems, software and platforms, there are additional roles and responsibilities including:

Information Governors

Information Governors are senior stakeholders accountable for ensuring that the information assets (including any nominated Monash IT systems, software and platforms) are managed appropriately under their governorship.

Information Stewards

Information Stewards are responsible on behalf of the Information Governor to implement and enforce comprehensive data management processes throughout the data life span, ensuring the quality of the information in Monash IT systems, software and platforms is maintained. This includes ensuring the data, information and records are accurate, complete, reliable, trustworthy, secure, and that all relevant relationships and context held within the systems, software and platforms are maintained and preserved for the full life span of the information asset.

Group Information and Records Management

Group Information and Records Management are responsible for establishing and managing the operational processes to support the Information Management Policy and the Information Governance and Recordkeeping Procedure.

Group Information and Records Management is also responsible for:

- providing direction and coordination of the Information and Data Management Assessments;
- developing and maintaining the Retention and Disposal Authority;
- authorising Notices to Delete;
- overseeing the archives collections and management processes;
- approving access requests to the University Archive collections;
- management and preservation of the physical and digital University Archives.

Information Management

Monash prioritises records of decisions and actions which are an essential source of information for effective and responsive University management.

The duty to document does not cease as Monash embraces new ways of improving its research, teaching and administrative functions, while constantly engaging with its staff, student and affiliate communities, including applying advanced data analytics and communicating through social media platforms.

For transparent and accountable administration, records of decisions, including the reasons for those decisions, need to be made and kept. This may include keeping new forms of evidence, such as data code or algorithms (including those related to AI activities).

The most significant records of the University are selected to form a part of the Monash University Archives. They tell the story of Monash and illustrate how the University affects, and is affected by its defined communities.

Well-managed information is the result of planned, enterprise-wide management of information assets, technologies, processes and staff behaviours. Information needs to be managed well within individual divisions and departments and across the University as a whole.

All actions provided in this Framework, either expand upon or provide additional information to the relevant sections of the Information Management Policy and the Information Governance and Recordkeeping Procedure.

Terminology

The policy uses the term ‘information asset’ to refer to records, information and data collectively and ‘information management’ to refer to their collective management.

For the purposes of this Framework, information assets can be in either hard copy or digital format and can roughly be divided into three main contexts.

Information Asset Categories

For the purposes of this Framework, information assets can be in either hard copy or digital format and can roughly be divided into three, mutually exclusive, main categories:



Locally managed	Collaborative spaces	IT Systems, software and platforms
Information assets held and controlled by individual information creators or consumers who are the only ones with knowledge about and access to the information. Examples include individual email accounts, individually owned Google Drives, a locked filing cabinet which is accessible to one person. Information about accessing various tools to create and manage locally controlled spaces can be found on the University’s eSolutions Service Desk webpage	Information assets held and controlled by a team of information creators or consumers. Examples include shared Google Drives, team share drives, file share files/folders, email role accounts, shared storage rooms/filing cabinets. Information about accessing various tools to create and manage collaborative spaces can be found on the University’s eSolutions Service Desk webpage	The University has many hundreds of different IT systems, software and platforms under its ownership and control. All of these various IT environments are constantly creating and managing the majority of the University’s digital information assets. Well known examples include: Callista/Banner, SAP, TRIM, UNICRM, PURE, Frevvo, however there are many others in use across different areas of the organisation. The way in which the data, information and records are held within these assets is determined and controlled by the relevant Information Governors and Information Stewards.

It is important to note, that due to the breadth and complexity of University functions and activities, undertaken at Monash University, it is likely that other types of information assets could exist outside the ones listed above.

In these cases, specific advice about how to manage the information asset should be obtained by contacting Information and Records Management directly at groupinformationmanagement@monash.edu

Information Management Lifespan Principles

All University information assets will have a lifespan. Not all information assets will pass through every principle, nor will every asset touch every principle in a linear fashion.

1. Created accurately and completely
2. Describe so they can be found and understood
3. Stored securely and preserved so they remain usable
4. Kept accessible for as long as needed by the University
5. Accountably destroyed when no longer needed
6. Available for reliable use and re-use by the University as required for business purposes

In the first section of this document, each of the above principles will be addressed in regards to how information assets should be managed at both a local level and within collaborative/team spaces.

The second section of the document will provide more details about the roles and responsibilities of Information Governors and Information Stewards. Although these roles incorporate the same six (6) Information Management Lifespan Principles, with the responsibilities and roles for Information Governors and Information Stewards outlined in detail.

Section 1: Information Management Lifespan Principles - Locally Managed & Collaborative Spaces

Principle 1: Create information assets accurately and completely

Whether it is the set up of a new folder in a collaborative space, or the procurement of a new Information business system, it is always important to consider the following questions when creating or capturing new information assets.

- Is the creation of this information necessary?
- Have I/we checked first if this information is being captured somewhere else in the University?

Regardless of where the information is created or captured, it is always important to be aware of the University's requirements around managing personal and or sensitive information. Monash University values the privacy of every individual's personal and health information and is committed to the protection of this information, and this applies no matter whether the information is being captured and created locally, collaboratively or in University information business systems.

The Monash University Information Security and Classification Management Procedure and the Information Classification and Information Handling Standard provide further, general guidance on safeguarding University information assets and University information.

Locally Managed

Individual work email accounts, the "My Drive" section in a Google Drive and even the "Desktop" area on a Monash issued computer can easily become full of information and records and as a consequence, require some management.

It is up to individual information creators to determine the best way to set up their own workspaces in these environments and to ensure that they are following the requirements as set out in the University's Information Technology Acceptable Use Policy. Some suggestions regarding titling and ongoing management of information held locally will be covered in the remaining principles of this Framework.

eSolutions also provides tips on using email filters and labelling as well as suggestions for getting started with G-Suite.

Collaborative Spaces

It is important to carefully consider how shared collaborative spaces will be used in both the short term and over time. Collaborative spaces should be managed purposefully. Examples of these spaces include:

- "shared email mailbox" (sometimes referred to as a group role account),
- "Shared drive" in the G-Suite, and/or
- file shares on an area's "S: Drive"

When thinking about the creation of any these collaborative spaces, you need to consider:

- What types of information is likely to be created or captured in the email role account, shared drive or S: Drive? To again question whether this information is already being captured elsewhere, or if this process is likely to end in the creation of unnecessary duplication of the same information.
- Who will need to access this information in the short term as well as longer term? Will access controls be necessary? If access controls are required, is further advice required about where to best store the information and how long it should be kept? Assistance on these matters can be provided through submitting an Information and Data Management Assessment form.
- Will information containing personally identifiable information be captured or created in these spaces, and if so, will this information be able to be managed in accordance with the relevant University Data Protection and Privacy requirements? An example of what not to do with personal information, can be explored in Case Study 4 - Jacob likes Birthdays in the Appendices.
- Is there a clear process for managing email role accounts and shared storage spaces? This is crucial to ensure continuity of ownership and management during any potential staff changes.

In addition, please note that eSolutions provides helpful technical advice and information, including how to set up email role accounts (see "shared mailboxes" and "Google drive" and "Data Storage" links for more information).

Principle 2: Describe the information asset so they can be found and understood

In addition to the relevant details outlined in the Information Governance and Recordkeeping Procedure, the following also applies.

Locally Managed & Collaborative Spaces

Where possible, use clear and easy to understand language (e.g. avoid acronyms that might lose their understanding over time) when:

- setting up your local email folders;
- and/or creating folders and new documents in "My Drive" or a computer's "Desktop" area.

Particular attention should be applied to titling information in the content of email and/or documents containing personally identifiable information.

For example, if working on a document locally that contains personally identifiable information consider adding a 'destroy date' to the folder title and include this in a relevant calendar note as a reminder to action later.

If there are draft documentation or working papers being managed in a collaborative space that duplicates information that will eventually end up being moved into an IT system once finalised, then the titling of the working spaces should reflect this where possible.

See *Case Study 1 - Celia Commences at Monash University* in the Appendices for an example of how this principle might be considered in practice.

Principle 3: Ensure the information asset is stored securely and preserved so it remains usable

As per Principle 1, regardless of where the information is stored, it is always important to be aware of the University requirements around managing personal and or sensitive information.

Locally Managed & Collaborative Spaces

In many instances, it may be necessary to create or capture certain information locally. Draft and working papers may logically begin their existence in locally managed spaces.

Storing drafts and working papers: As noted above, once information moves from being in draft/working paper stage to final and/or approved stage, it is important that the final/approved information is moved into the most appropriate University IT system for longer term storage. The most appropriate University IT system should align to the function/activities and business processes of each area across the University. For example, HR records and information usually reside in HR systems, software and platforms, Finance records and information usually reside in Finance systems, software and platforms and so on. If you are unsure about what University IT systems your area uses, it would be recommended that you first seek advice from your local supervisor/manager.

Storing information and records in the most appropriate University IT system long term enables the information to be managed securely as well as ensuring that University information is accessible over time. It can be difficult for colleagues (both now and into the future) to find or access important University information that has been stored locally by an individual Information Creator/Consumer, especially if that individual has left the organisation. Principle 4 provides more information on determining when information should be moved into University IT systems.

Longer term storage: Many collaborative spaces such as email, G-Suite options and file shares such as S: Drive are not considered suitable long term storage options for University information or records. From a practical perspective, this may negatively impact the security and accessibility and useability of the information over the longer term.

While University IT systems have Information Governors and Information Stewards to help manage them over time, collaborative spaces may only have individual Information Creators looking after them. If individual Information Creators change roles or leave the University, those spaces (and the information and records contained within them) may end up becoming orphaned, forgotten about and later lost over time.

However, in practical terms, there may be situations where certain activities and processes can only be managed in these spaces. If this is the case, and depending on the kind of information being stored in the collaborative space, it may be advisable to seek additional advice, especially if:

- the information being managed in the collaborative space, is related to an existing Monash business process/procedure/service;
- the collaborative space contains personal and/or sensitive information;
- the collaborative space will become the primary repository for the information (and the information is not available anywhere else).

Additional advice can be obtained by submitting one or all of the following assessments (depending on what is relevant):

- Information Security Risk Assessments (ISRA)
- Privacy Impact Assessments (PIA)
- Information and Data Management Assessment (IDA)

It is essential that in addition to seeking this assessment advice, that individual Information Creators responsible for the collaborative spaces transfer ownership to the appropriate manager or delegate when changing roles within the University as well as when exiting the University.

Exiting the University - Human Resources provides a detailed checklist for staff who are exiting the University. In regards to information management, this checklist notes that staff who are leaving the University are required to reassign ownership of any email role accounts, shared drives, google drives/sites to a nominated Monash staff member (or delete the site or data in accordance with Principle 5).

Principle 4: Kept accessible for as long as needed by the University

When considering storage options, outside of managing privacy and security concerns, the next most important aspect that should be driving these decisions, involves ensuring the information is accessible to whoever requires access to it, for the purposes of the business.

Locally Managed & Collaborative Spaces

To help determine when information should be moved into a University IT system (out of a locally managed or collaborative space) the following questions should be considered:

- Does the information record evidence of a business decision?
- Does it show how a transaction occurred?
- Does it show how a decision was made?
- Does it relate to an assessment or investigation?
- Does the record demonstrate when or where an event happened?
- Does it indicate who was involved or what advice was provided?

If the answer is YES to any of the above questions, then the records belong in a University IT system.

Other types of information or records that belong in a University IT systems include:

- those which add value to an existing record and/or are needed to clarify, support, or provide context to an existing record;
- draft agreements containing legal advice which form part of contract negotiations;
- any formal draft of a policy, cabinet submission, agreement or legal document;
- records required to protect rights and entitlements of individuals, groups, or the Government;
- records and information that may be of cultural or historical value to the University and/or the wider community.

In rarer cases, the following types of information and records may also need to be retained for varying lengths of time and should also be moved out of locally managed areas including records and information that:

- are required in a current or has been identified as being required in a future legal proceeding. This includes any civil or criminal proceeding or inquiry where evidence may be given before a court or person acting judicially such as a Royal Commission or Board of Inquiry;
- are required for meeting any Freedom of Information (FOI) applications which are not finalised;
- are required for an audit or investigation which is not yet finalised; and/or
- are subject to a disposal freeze applied by the government or the University.

If you are still unsure of what University IT systems your records or information belongs to, please contact Information and Records Management for a consult/request for guidance and support groupinformationmanagement@monash.edu.

Is TRIM the preferred option when moving information assets held locally and/or in collaborative spaces/team areas?

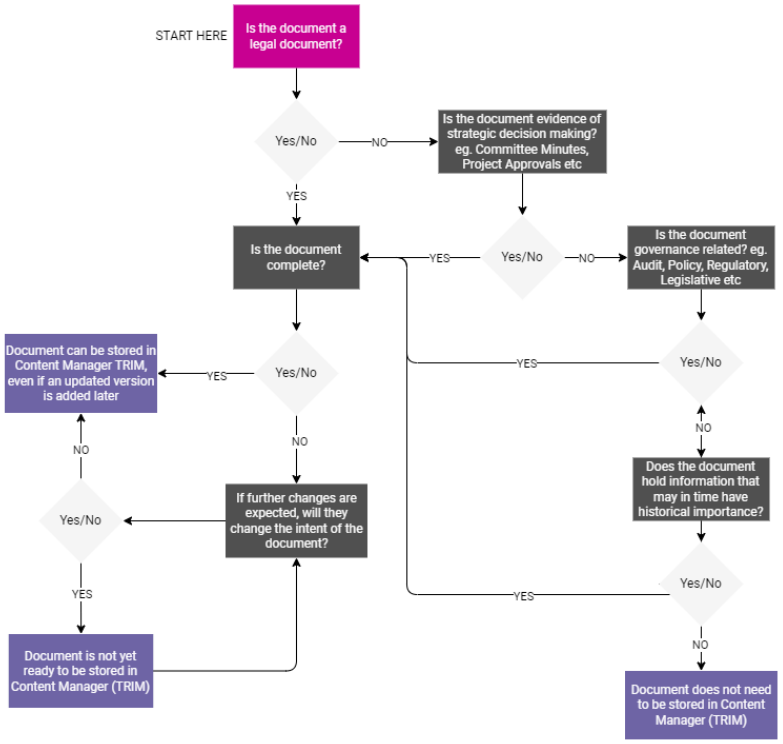
In some cases, if there are no other suitable options, TRIM may be an appropriate long term storage solution for information and records that don't logically belong in any other University IT system.

TRIM (known commercially as OpenText Content Manager) is the name of the University's records management system. It is an enterprise system widely used in areas across the University, and manages short and long term records, as well as permanent records. TRIM captures and maintains Monash's corporate memory and necessary business information. TRIM has the ability to manage different types of records, separately, but within the one system. Therefore, confidential files can easily be restricted to selected user groups. TRIM also has a sophisticated audit log system, and can quickly identify which user accessed which records when, and can document what the user did to the records (e.g. whether they simply viewed the records, printed them, moved them etc.)

However, it is important to note that there are limitations in terms of the types of formats that can be stored within TRIM (for example, TRIM cannot be used for the storage of databases). In addition, there are additional restrictions in terms of the content of the records/information that is accepted into TRIM.

Additional information about TRIM can be located here, the following decision tree also provides some guidance on when documents should be going into TRIM.

Content Manager (TRIM) Decision Tree - When should a record be stored in TRIM?



Principle 5: Accountably destroyed when no longer needed

Locally Managed & Collaborative Spaces

Identifying information and records with short and long term value: any records that fall under categories listed under the University's Retention and Disposal Authority need to be retained in accordance with the relevant sentencing requirements as identified in the Authority. If in doubt, and you can provide a high level summary of the types of records information (and/or the University activities that the records and information relate to, you can request advice about how long to maintain the information and records by submitting a Information and Data Management Assessment. Such an assessment is only applicable to groups of records and is less useful for individual records or a large collection of different types of records/information or where the nature of the records/information is unknown.

Information and records have been previously assessed via an Information and Data Management Assessment (IDA) and/or ISRA and PIA. In which case the advice provided in those assessments should be followed.

Deletion under Normal Administrative Practice - Routine deletion: For documents that may eventually end up in Monash IT systems, software and platforms, it is important to routinely remove the duplicated working copies from the locally managed area, once the activity has been completed. These kinds of documents can usually be deleted under the provisions outlined under Normal Administrative Practice (NAP) processes. This might become relevant when downloading and reviewing applicant information (e.g. resumes) as part of job recruitment processes.

Normal Administrative Practice (NAP) refers to the principle that certain records do not need to be captured into official recordkeeping systems and may be destroyed without formal authorisation.

NAP applies to all information and data formats and balances efficiency with responsible information management. It complements, but does not replace, the Monash University Retention and Disposal Authority (RDA), by allowing individuals and organisational units to identify and manage their own low risk records. Under NAP, low-value, short term records created, acquired or collected during the course of normal business activities can be deleted without formal authorisation.

NAP is an important tool in the efficient and accountable management of information and should be applied regularly as part of normal working practices. A clear, well supported and widely distributed NAP procedure reduces the risk of inappropriate destruction as well as ensuring non-essential information is not over retained, particularly important when information is highly sensitive and sensitive. A consistently applied NAP also contributes to strong information governance and efficient work practice by prioritising the retention of critical information while disposing of non-essential material.

All staff should be familiar with and understand NAP to ensure that it can be applied correctly in their day-to-day work.

Facilitative records described below are pre-authorised for destruction by the Public Record Office of Victoria PROV (PROS 22/04 Disposal Standard) under Normal Administrative Practice (NAP) principles:

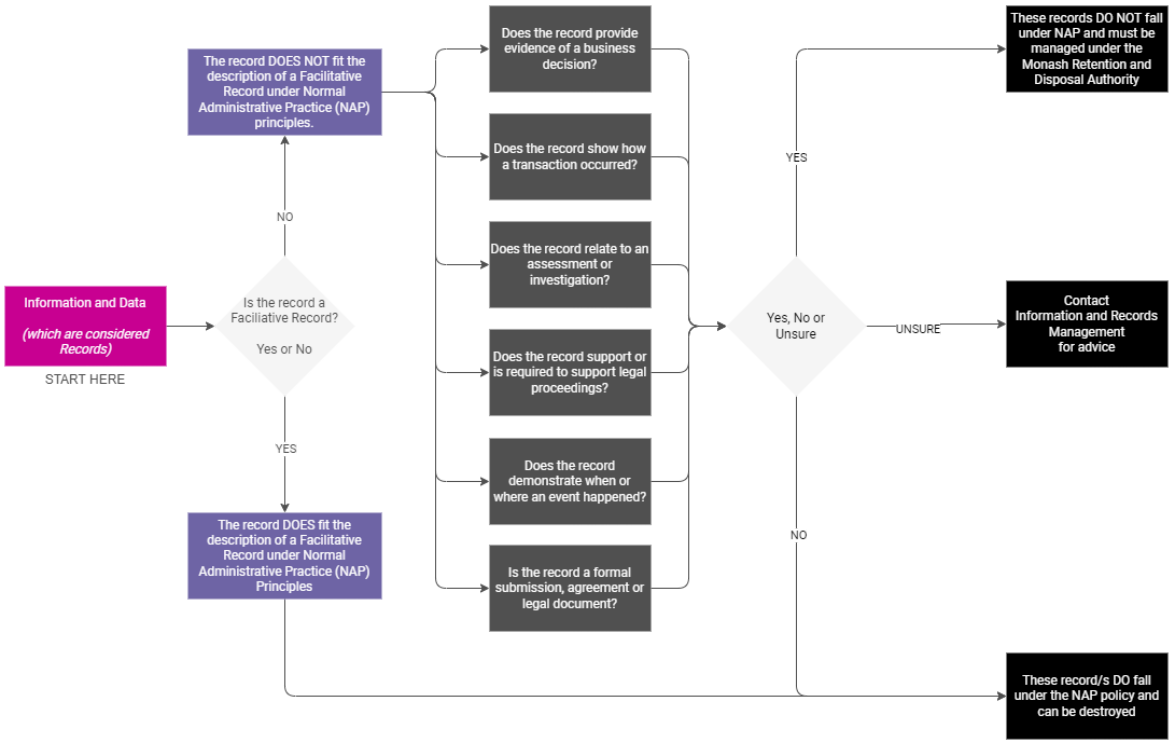
- working documents, such as notes or rough calculations used to assist in the preparation of other records (e.g. reports and statistical tabulations);
- working papers or background notes used to develop drafts;
- spreadsheets or word processing documents that have been incorporated into correspondence or a separate final document;
- minor drafts and transitory documents, where the content is reproduced elsewhere and the information will not be needed to show how the work has progressed or actions approved;
- draft and transitory documents that do not contain significant or substantial changes or annotations;
- draft and transitory documents that are not required to document business activities;
- minor updates of content, such as those in databases, which will not be needed to show actions, decisions or approvals;
- communications for the purpose of making minor arrangements;
- duplicate copies of information that already exists in a University enterprise system eg: information download from, or uploaded to, Callista or SAP;

- Emails, which may be located in either a personal mailbox or a University role account, that have been saved to and/or processed in a University enterprise system;
- duplicates of publications and promotional material;
- periodic backups of records, information, data, software and settings for recovery in case of technical failure and/or catastrophe and are duplicate copies of official business records/data that is held elsewhere on a managed system.

It is up to Individual Information Creators and Consumers to routinely undertake the necessary steps to maintain their locally managed areas and to ensure that routine reviews and any necessary follow up actions from those reviews are undertaken as required.

The following Normal Administrative Practice Workflow Diagram may be a useful resource when undertaking such reviews of locally managed areas.

Normal Administrative Process (NAP) Deletion Assessment



Principle 6: Available for reliable use and re-use by the University as required for business purposes

Locally Managed & Collaborative Spaces

If all of the Principles 1-5 are being followed, then all relevant University records and information assets that are required to be accessed by University consumers, should be found in the relevant University IT system. The management of those University IT systems are under the control of the relevant Information Governors (see Section 2 for more information).

Relevant Cyber Security controls and personal data protection requirements must be adhered to when sharing records and information across the University from locally managed and collaborative spaces.

Section 2: Information Governor and Information Stewards Roles and Responsibilities

Information Governors Role

The Information Governor is the senior stakeholder accountable for ensuring that the asset under their governorship is compliant with the university data policies and standards. If Information Governors have components of their information assets stored in locally managed or collaborative spaces they are advised to follow the principles outlined in Section 1 of this Framework.

The requirements outlined in this section of the Framework are primarily focused around the management of information assets that reside in IT systems, software and platforms that are being managed at an enterprise level and support the functions and activities of core University business (e.g. learning and teaching, research, student management, governance and risk, etc).

See https://sites.google.com/monash.edu/data-at-monash/enterprise-data-governance/people for examples of Information Governor and Information Stewards and their related entities.

Information Governors Responsibilities

This section is broken down into two parts. The first relates to the responsibilities of an Information Governor when decisions are being made around creating new information assets, including new IT systems, software and platform solutions for information assets under their control. The second part relates to ongoing responsibilities for established information assets, including IT systems, software and platforms.

Part A: Developing New Information Assets

When making decisions about creating new information assets, extending existing information assets and procuring new IT systems, software and platforms to capture and manage new information assets, the following requirements should be adhered to.

1. Check that there are no existing solutions already in place across the University that could be leveraged to meet the requirement.

   Some initial resources to investigate include:

   - University Archives Information Asset Registry
   - University Approved Software Catalogue (eSolutions) and Software Information (eSolutions)
   - Cyber Security Approved Services (eSolutions)
   - Data Storage (eSolutions)

2. Ensure that any new information assets are able to comply with all relevant Monash policies and procedures. Initial advice to consider in regards to this requirement may be found in the relevant domain or functional area of the University's Policy Bank, as most University policy will reference the relevant regulatory requirements for that domain or function.

3. When using internally or externally provided technologies/ infrastructure the following factors should be considered at the beginning of the process.

   For every relevant information asset, under the custody of the Information Governor the following requirements should be adhered to: both at the start and throughout the lifespan of that information asset.

   - Maintain Information asset security (tailored advice can be provided via relevant Information Stewards completing an Information Security Risk Assessments).
   - Maintain privacy and data protection of the information asset (tailored advice can be provided via relevant Information Stewards completing a Privacy Impact Assessments (PIA).
   - Be able to facilitate the University's mechanisms for authorised and complete record destruction and prevent any unauthorised disposal. Most information assets can be assessed for this purpose at the beginning of the process. Monash University has a detailed Retention and Disposal Authority which outlines how long different types of information and records need to be retained for. Understanding these requirements at the beginning of any new IT system, software or platform implementation process ensures that disposal can be built in at the beginning. Tailored advice can be provided via relevant Information Stewards completing an Information and Data Management Assessment (IDA).
   - Ensure the longevity and reliability of the information asset is maintained: ie: ensure access is stable and there is a long-term viability of the systems/solutions to ensure continuity of service.
   - Ensure the authenticity and auditability of the information asset: IT systems, software and platforms should offer means to demonstrate the authenticity of data and enable audit trails for accountability.
   - Protect all copyright and proprietary interests held within the information asset: e.g. ensure measures are in place to protect against unauthorised use or infringement of proprietary data.
   - Ensure the information asset has appropriate retrieval and extractability capabilities: Verify the ease and reliability of retrieving records (including data) while it's stored in the system/solution (including for cloud) and ensure the ability to extract records in case of service discontinuation.
   - Ensure the information asset can maintain accessibility and continuity: e.g. ensure seamless access to records for the University is maintained with consideration for fulfilling obligations related to Freedom of Information (FOI) applications, inquiries, Royal Commissions or other legal requirements.
   - Be aware of and ensure about any data sovereignty and governance requirements for the information asset in regards to where and how the information assets are to be hosted, ensuring arrangements to safeguard that data is held in accordance with legislative requirements. Consider potential foreign legislative, regulatory or administrative obligations for foreign-owned companies that may impact the security and accessibility of University information assets in both the short term as well as over the full lifespan of the information asset.

Part B: Managing Information Assets

Data integrity and metadata maintenance

4. Ensure data remains intact and unaltered, including the maintenance of metadata for proper context and accuracy. Where possible, metadata should be able to be tagged to help with identifying data for future actions (be it deletion, extraction, etc). The Information Governor is therefore:
    - Accountable for making sure that the right data definitions are in place
    - Accountable for the quality of data for their data asset
    - Ensure that their data asset is appropriately classified according to applicable Data Privacy policies.
    - Take corrective actions to address the data quality issues, and ensure that a data quality reporting mechanism exists.

A tool to assist Information Governors with the execution of their responsibilities around the use of metadata and data is the Data Reference Model which has been developed using agreed terminology and key concepts that are important to the business of Monash University.

The Higher Education Data Reference Model describes a standard set of Data Architecture elements relevant to higher education. It was created by CAUDIT, an industry group for information technology in higher education. It is used to identify who is responsible for governing the data, so that stewardship responsibilities can be incorporated into these roles. The model has been tailored to reflect functions that are specific to Monash University after receiving suggestions on modifications and additions/ deletions from directors and leaders in the portfolios and faculties in 2022. The model will be updated periodically.

Additional information can be found within the Enterprise Data at Monash - intranet site for enterprise data governance

Ongoing compliance responsibilities for information assets

If the information asset was established following the requirements outlined above in Section A, then decisions (including long term decisions) about the storage and preservation of the information assets should have already been made and documented. However, if there are changes to how the information asset is being managed, then a review is required and appropriate advice should be sought via new;

a. Information Security Risk Assessments (ISRA)
b. Privacy Impact Assessments (PIA)
c. Information and Data Management Assessment (IDA)

Access to Information Assets

As outlined in the Information Governance and Recordkeeping Procedure (and repeated here for convenience),

Access to records must be available to authorised personnel to enable:

- prescribed activities for Monash to occur, subject to satisfying any requirements or conditions; and
- information to be shared between relevant organisational units.

Access to shared storage systems must be limited to individuals with approved access and permissions within the Monash environment.

- PEN (Enterprise Data Lakehouse) Access is granted under the conditions outlined in the User Access website
- Power BI Access is granted under the conditions outlined in the User Access website

Access to Monash data must be limited to authorised personnel to protect:

- the privacy of staff, students and other affiliated persons (including prospective students and alumni);
- confidential, restricted or sensitive information; and
- information subject to legal professional privilege.

Any person wishing to request a document under a Freedom of Information Request may do so. A request must be in writing, accompanied by the application fee as set by government regulations and published on Monash's Freedom of Information website. All requests for access to documents must be sent by email to foi@monash.edu or by post and addressed to: The Freedom of Information Officer, Monash University, VIC, 3800.

Staff must provide immediate access to information subject to a Freedom of Information Request to authorised personnel, with the information protected from:

- modification;
- unauthorised use; or
- unauthorised destruction.

All staff can request access to material in the custody of Group Information and Records Management. Archival records are made available for research purposes to staff, students and external researchers in the reference area by appointment. Publicly available records such as Council minutes, annual reports, calendars and faculty handbooks are also available for use in the University Archives.

Group Information and Records Management must consult with relevant areas if an access request covers records that may:

- be commercially sensitive, commercial-in-confidence, or contain a legal opinion;
- contain personal or sensitive information;
- be under embargo and/or University Council and associated committees confidentiality;
- jeopardise future investigatory functions or law enforcement, or threaten the safety of any person and/or could compromise Monash security if disclosed, such as the location of CCTV, data centres, chemicals etc; and
- contain culturally-sensitive Indigenous information.

Access requests may be declined after consultation with the relevant area if the records meet one or more of the above criteria.

Access requests may also be declined if the age and/or condition of the records renders them incapable of being accessed or if the storage area is unable to be accessed.

Disposal and Retention of information and records held within information assets

Detailed information about determining how long records held in information business systems are determined by the relevant information assets Information and Data Management Assessment IDA).

What is an Information and Data Management Assessment?

In order to help staff understand what their information management responsibilities are, it is important that when systems or activities involving information are created or even reviewed, that an overview of this detail is provided to Information and Records Management. Completing this assessment (by completing this form) allows for Group Information and Records Management to help staff manage the breadth and scale of information being captured and managed across the University.

Please refer to Appendix 2 "How appraisal and sentencing work" for more information about how information, data and records are assessed by Group Information and Records Management.

At the end of the assessment respondents will receive a copy of their questionnaire responses, and confirmation from the Group Information and Records Management that the Information and Data Management Assessment is complete.

Additional action will only be required after the Information and Records Management team have reviewed the assessment responses and deem that an additional follow-up consultation is required.

What is the Notice to Delete process?

As a public agency, the University must comply with the Public Records Act (Vic 1973) and undertake regular disposal activities to ensure the proper destruction of University records in accordance with legislation. Disposal activities within the context of Monash refer to the authorised deletion/destruction of records.

The Monash University Retention and Disposal Authority (RDA) provides information about the minimum amount of time that Monash must retain its records. It is crucial that the requirements are adhered to in order to ensure that records are not retained longer than is necessary, nor destroyed too early.

Group Information and Records Management identifies Monash information that meets the criteria for the authorised deletion of records via an Information and Data Assessment (IDA). In some instances, an IDA will lead to a formal Notice to Delete (NTD) being issued to the relevant Information Governor for approval and action.

When will an IDA lead to an NTD?

Not all IDAs will require an Notice To Delete (NTD).

A Notice to Delete will only be issued when records meet the following criteria:

- are high risk according to the Public Record Office Victoria (PROV) High Risk/High Value (HRHV) assessment matrix (see below)
- contains personal identifiable information (PII) that is classified as sensitive or very sensitive according to the Monash University Information Confidentiality Classification Levels.
- the records are currently over retained OR are within 6 months of being due for disposal.

Information and Records Management will notify the relevant Information Governor if an Information and Data Management Assessment (IDA) requires a NTD to be issued.

Information and Records Management maintains the discretion to determine when an IDA requires a formal NTD is to be issued.

However, any staff member may indicate that a Notice To Delete is required when submitting an IDA form.

Additional information for Notice to Delete actions

In accordance with the University's Information Management Policy, all Notices To Delete (NTD) must be authorised by the University's Archive Manager and approved by the Director of Information and Records Management.

All Notice to Delete statements will be issued to the relevant Information Governor via Information and Records Management. The Information Governor is responsible for ensuring that the details in the Notice to Delete are communicated to the relevant Information Steward and technical teams to action.

The Information Governor/Information Steward is responsible for notifying Information and Records Management that the deletion action has been completed.

A request to retain any records identified in a Notice to Delete (NTD) must be submitted to the University Archives Manager via the groupinformationmanagement@monash.edu email account and must include business reason to justify the records being kept.

Information and Records Management will maintain a record of all IDA and NTD activities, including a final verification that any required deletion/removal of information actions have been completed.

When a Notice to Delete is required, but at a later point in time.

When an Information and Data Assessment (IDA) has been issued, and the records fit all of the criteria noted above, EXCEPT the records are required to be retained for another 6 months or longer, it is up to the relevant Information Governor and Information Steward to keep track of when the necessary retention period has been completed.

Once the records become due for legal disposal a Notice To Delete (NTD) will be required. The Notice To Delete provides the necessary approval for the disposal of data for which Monash is the legal custodian, under the Public

Records Act (Vic) 1973. To initiate the Notice To Delete process, please contact Information and Records Management at GroupInformationManagement@monash.edu.

Will the disposal advice in an IDA always require a NTD to be issued?

A Notice to Delete will NOT be required for:

- duplications of records, especially duplications of records, where the source information has already been deleted under a Notice to Delete (or will be in the future). Under Normal Administrative Practice (NAP), duplicates meet the criteria for NAP and only require an IDA to action.

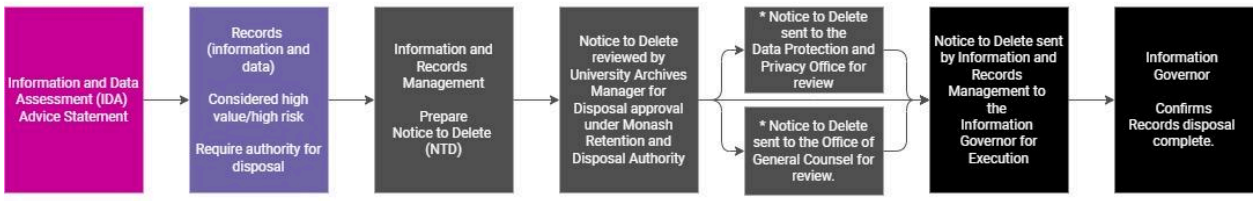
What happens when an IDA contains disposal advice, but an NTD is not required?

The Information and Data Management (IDA) statement will contain information about when the deletion of the records is due to occur.

When a Notice to Delete (NTD) is NOT required, it is the responsibility of the Information Governor to ensure that documentation of all information (including records) destroyed is being maintained, including descriptions of records, date ranges, destruction dates, and authorisation.

It is the responsibility of the Information Governor/Information Steward to always ensure that the information provided for the IDA assessment is accurate, and if at any point in time, any significant changes occur to the information covered by the IDA, then a new IDA request form must be completed.

Notice To Delete pathway



** The requirement for Notices To Delete to be reviewed by the **Data Protection and Privacy Office (DPPO)** and the **Office of General Counsel (OGC)** is determined on a case by case basis.*

High Risk/High Value and Notice to Delete

In the context of Monash University, Group Information and Records Management uses appraisal techniques for a variety of purposes, but the most prominent of these relates to using appraisal techniques as part of the process for applying the sentencing outlined in the Monash University Retention and Disposal Authority (RDA). Appendix 2 contains more information about how high risk/high value appraisal and assessment of records is practiced at Monash.

Information Stewards Role

Each information asset (most likely to take the form of Monash systems) may have one or more Information Stewards depending on the complexity of the information asset.

Information Stewards are therefore required to undertake specific tasks at the creation stage as delegated to them by the relevant Information Governor.

Information Stewards Responsibilities

Each information asset will require the following information governance measures to be completed:

Data integrity and metadata maintenance

1. The Information Stewards are tasked with the following data quality responsibilities
    a. implementation and enforcement of data management processes;
    b. take corrective actions to address data quality issues and address any gaps in the processes on behalf of the Information Governor;
    c. manage data assets through the entire data lifespan (creation, access, usage, sharing, preservation or deletion) to maintain their quality, integrity and consistency and to avoid duplication of data;
    d. define data quality rules which define what is considered as good quality data, and are responsible for maintaining quality;
    e. maintain quality metadata of the data asset for which they are responsible, in the enterprise data catalogue platform;
    f. maintain awareness of the Data Protection and Privacy policies as created by the Data Privacy office for the maintenance of the data.

    Detailed advice around maintaining data quality can be found on the Data Governance website, in particular the Data Reference Model.

Ongoing compliance responsibilities for information assets

2. The Information Steward is responsible for submitting the following assessments on behalf of the Information Governor and ensuring any follow up tailored advice and/or requirements are included at the creation/set up stage of new information assets (in particular new information business systems) including the;
    a. Information Security Risk Assessments (ISRA)
    b. Privacy Impact Assessments (PIA)
    c. Information and Data Management Assessment (IDA)
3. It is the responsibility of the Information Steward to ensure the advice provided in these assessments is reviewed annually and potentially resubmitted to ensure the advice is still current, after any significant changes have been made to the information asset.
4. It is responsibility of the Information Steward to ensure that any advice regarding how long the data needs to be retained for is tracked in the system and that a new Information and Data Management Assessment is submitted prior to data becoming due for retention, so the appropriate checks can be made before a Notice to Delete can be issued to the responsible Information Governor for actioning.

Please note that an Information Steward can request a Notice to Delete to be prepared, via an Information and Data Management assessment, however Notice to Deletes will only be issued to the Information Governor, by Group Information and Records Management, for authorisation and action purposes.

5. The Information Steward will coordinate the technical steps required to implement a Notice to Delete process and instruct technical teams responsible for updating Information and Records Management via email when disposal is completed. It is also the responsibility of the Information Steward to update and keep track of what has been deleted in the relevant information assets Data Management Plan.
6. It is recommended that Information Stewards (in consultation with the relevant technical teams involved with managing the information assets, create and maintain a Data Management Plan for each information asset. It is recommended that any advice provided through Information Security Risk Assessments (ISRA), Privacy Impact Assessments (PIA) and Information and Data Management Assessments (IDA) are kept alongside the information assets Data Management Plan (or linked from it).

Appendix 1

Glossary of Terms

Associates	For the purposes of this procedure, ‘associates’ are defined as contractors, conjoint appointments, affiliates and adjunct appointees.
Public records	A public record is defined as any record made or received by someone working for Monash in the course of their duties. Records can be either hard-copy (such as a paper file or a register) or electronic (such as a database, digital file or email). All University records are considered to be public records under the Public Records Act 1973. Under this legislation, 'record' means a 'document' as defined under the Evidence Act 2008.
Record	Information in any format created, received, and maintained as evidenced by Monash, in pursuant of legal obligations or in the transaction of business.
Sentencing	Sentencing is the process of identifying and classifying records according to a disposal authority, recording the appropriate disposal decision and action for the records, and applying the disposal actions specified in the disposal authority.
Business information system	Refers to databases, geospatial data systems, human resources systems, financial systems, workflow systems, client management systems, and electronic document and records management systems (EDRMS).
Legitimate Business reasons	These are reasons identified as being genuine reasons why records need to be retained beyond their designated disposal sentence. *Examples are: records are used as part of business decision making; records are included in ongoing contract negotiations; records are the subject of FOI requests or subpoenas; the records are in scope for current legal proceedings.*

Appendix 2

How sentencing and appraisal works

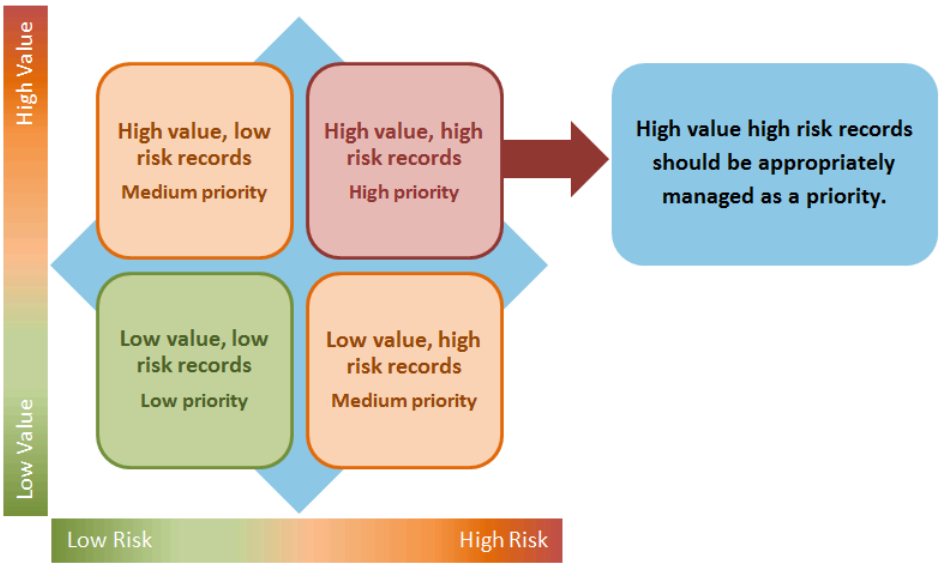
Appraisal is a recognised recordkeeping concept

As noted by the Public Records Office Victoria, it is a theoretical technique that involves "evaluating business functions and activities" and it is taught to recordkeeping practitioners as part of their professional training.

In the context of Monash University, Group Information and Records Management uses appraisal techniques for a variety of purposes, but the most prominent of these relates to using appraisal techniques as part of the process for applying the sentencing outlined in the Monash University Retention and Disposal Authority (RDA).

This can be achieved through an accepted practice known as HRHV (high risk, high value). By identifying records that are of high value or which are at high risk, Monash University can ensure that these records are well managed and are allocated appropriate resources and strategies.

In many ways, the HRHV proposition, when used in conjunction with the sentences for retention and disposal as outlined in the Monash RDA, accommodates for the multiple views/uses of records but at the same time, ensures that sentencing decisions always favour the University's best interests, over say a personal staff member or team beliefs and values.



Source - https://prov.vic.gov.au/recordkeeping-government/a-z-topics/high-value-high-risk-records

Again, it is important to note that the HRHV proposition is primarily used as a recordkeeping tool to aid in appraisal and sentencing processes.

Although the term "value" is open to interpretation, within the recordkeeping context, in simple terms, "high value" refers to records that are of value to the University Archives *(which in turn mean they are of value to both Monash University and the State of Victoria)*. Records that are sentenced as having "permanent value" are in effect the most highly valued to the University.

This doesn't diminish the business value of records either. The decision around what has high "business value" to the University will be more subjective and will depend on factors outside of the control of recordkeeping professionals.

However, in most cases something of high business value to the University, is likely to be already covered by the appropriate recordkeeping sentencing requirements in the RDA, as most core functions and activities undertaken by the University are included in the Monash RDA.

Examples of how different types of records are managed

Type of records	Risk/Value Status to the University	Likely period records need to be retained for.
Database containing staff names, addresses and birthdates created for non-business relevant reasons.	LOW VALUE / HIGH RISK	Destroy immediately after business use concludes
Archives collection of University photographs	HIGH VALUE / LOW RISK	Retain permanently in the Archives
Copy of email sent to student notifying them of admission results	LOW VALUE / LOW RISK	Retain for 30 days after email sent out, then destroy
University Council Minutes	HIGH VALUE / HIGH RISK	Retain permanently in the Archives

Appendix 3

Case Study Examples

While the instructions and tables in this document provide a useful starting point for understanding key recordkeeping and information management concepts, they can be challenging to relate to real-life scenarios encountered in day-to-day business. The following fictional cases are based on real-life examples but have been de-identified and created for educational purposes. They do not depict any specific person, event, team, or scenario

Case Study 1 - Celia Commences at Monash University

Celia has commenced a new administrative role within a central University area at Monash University and has been provided access to a work related Monash Gmail account as well as her team share drive in Google.

As part of her new role, Celia will be responsible for the agenda and minutes of an executive committee as well as managing future divisional events. She is unsure where to store the Faculty Governance committee records, but her team suggests that she continues to manage them in Google Docs where they are currently stored. Celia recalls from previous experience that committee papers need to be kept permanently and questions whether Google Docs is the best option. Celia decides to seek advice from Information and Records Management and submits an Information and Data Management Assessment request noting that she is managing both committee papers and events documents

Information and Records Management, as part of their formal, written response, advises Celia that, whilst Google Suite is acceptable as a *short term* location for access and collaboration purposes, University records requiring longer term retention should be uploaded into a University enterprise system such as Content Manager (TRIM) . As Faculty committee papers are an important source of information, particularly around decision making, they are considered high value/high risk records to be retained permanently . The use of Content Manager (TRIM) as a repository for governance committee records allows Group Information and Records Management to manage these records in accordance with long term preservation guidelines, ensuring that they also remain accessible to authorised parties across the wider University.

Celia shares this advice with her team and they implement a new process, agreeing on a timeframe to routinely remove old committee records from Google Drive once the master version is in Content Manager (TRIM) using Normal Administrative Practice NAP guidelines.

Advice relating to events documentation is also provided in the response by Information and Records management. As Celia has indicated that she plans to use the email role account to provide communication updates to event participants and will manage other event related information separately in other University systems, Information and Records Management are able to provide tailored sentencing advice for each possible component of an event ie. Financial data, OHS data

Case Study 2 - Bert is Decommissioning a Redundant IT system

Bert works in a technical systems support role within Monash and has been asked to decommission a system that has recently become redundant. He doesn't know a lot about the data held within the system, as his role focuses on the technical aspects of getting the system taken down, but he does know that he cannot delete University information without appropriate approval. Bert reaches out to the Information Steward for this system who confirms that approval has been sought and an Information and Data Assessment request has been submitted.

Information and Records Management are able to confirm in the subsequent assessment response that, although the data in the system is the 'source of truth', at 10 years old it is beyond the legislative retention period for the type of data it is and can be deleted. In addition to the written advice provided by Information and Records Management, the threshold for an authorised Notice to Delete is met and this is also provided to the Information Governor of the system for final approval. Once received, a copy is provided to Bert who can now commence decommissioning the system now he has the official approval to go ahead with the decommissioning process

Case Study 3 - Raj Hits his Email Quota

Raj has been an employee at Monash for nearly 30 years, in a number of various roles. Over the years, he has accumulated a vast number of emails, some dating back a decade, as he often goes long periods without deleting any. Given that his job frequently involves receiving large email files with videos and images, Raj has become increasingly concerned about reaching his email quota. This concern has led him to consider deleting some of the older emails to free up space but he is unsure whether he should do so.

After seeking advice from Information and Records Management, Raj discovered that his method of downloading images and videos from each email and organizing them by date and year in his Google Drive was causing him to retain duplicate records. Feeling more confident, he began deleting emails older than 12 months that contained these duplicate attachments, following Normal Administrative Practice (NAP). Raj also decided that it would be more efficient to perform regular deletions at the end of each year. With the new knowledge he gained, he could now identify which records could be deleted under NAP and which ones required further assessment or a longer retention period

Raj had a collection of photographs showcasing various campus buildings from the early 2000s, captured during a series of projects he worked on at that time. Through his engagement with the Information and Records team, Raj discovered that he could transfer these legacy items to the University Archives. The Archives would not only store them appropriately but also ensure they remained accessible. The Archives team was thrilled with this new photograph collection, and Raj felt proud to contribute to Monash's history in such a meaningful way

Case Study 4 - Betty likes Birthdays

Betty works in a University department and has compiled a small database of faculty staff, both current and retired, including their full birth dates and addresses. She enjoys surprising staff members by sending flowers to their homes on their birthdays so did not seek permission when collecting and managing this information. In fact, no one knows how Betty was able to acquire such personal information.

Although Betty may consider her database to be high value/low risk, its existence poses a significant risk to the University. The database serves no business purpose and the potential consequences of a breach, including the misuse of personal information, are high

Therefore, the University’s HRHV (High Risk, High Value) value proposition for managing these records takes precedence over Betty’s LRHV (Low Risk, High Value) value proposition. Betty would be required to delete the database immediately