INFORMATION GOVERNANCE AND RECORDKEEPING PROCEDURE

SCOPE

This procedure applies to all Monash staff and associates who handle information assets (records, information and data) in any format at Monash.

For the purpose of this procedure, 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).

PROCEDURE STATEMENT

This procedure outlines the governance roles and responsibilities, and practices that guide the creation, storage, access, and disposal of all information and information assets (records, information and data) across Monash. The procedure supports the application of the Information Management Policy and guides the framework for information governance at Monash.

This procedure applies to all Monash information assets, excluding research information assets, and all information contained within those assets, regardless of format, location, or means of storage. Recordkeeping includes all activities that impact the decision to create records, their management throughout various contexts of creation and use, as well as their preservation or destruction based on ongoing needs.

1. Records

1.1. Records of Monash's decisions and actions are an essential source of information for effective and responsive management as well as being required for legal and evidentiary purposes.

1.2. All Monash records, including paper documents, electronic files, photographs, maps, films, sound recordings, and emails, are considered public records.

1.3. Digital Monash records are stored in information technology (IT) systems, software, and platforms, including emails, social media, shared drives, and collaborative environments. Records can exist on different platforms and be stored on local servers or in the cloud.

2. Lifespan Information Management

Capture, collection and creation of information

2.1. The capture, collection or creation of information by or on behalf of Monash must:

2.1.1. accurately reflect the context and entirety of the activity that it records;

2.1.2. consider the primary purpose and potential secondary uses for the information, within the limitations set out by any applicable legislation;

2.1.3. comply with applicable confidentiality, data protection and privacy, and security requirements; and

2.1.4. ensure the accuracy and quality of the information at the time of recording.

2.2. When creating and managing information within applications, including word-processed documents, spreadsheets, presentations and desktop-published documents:

2.2.1. naming conventions should be clear, concise and consistent to facilitate easy identification, retrieval, and management of records.

2.2.2. redundant, obsolete, duplicate documents, as well as those with low operational or recordkeeping value, should be routinely deleted from email, file-hosting services and collaborative environments, following the Normal Administrative Practice process.

2.2.3. records or information that form part of a record should be registered or captured in the approved IT system, such as a Monash shared storage system (see the Approved Services List for guidance).

2.3. Where records with long-term/permanent value are identified, staff should seek advice from the University Archives about their long-term storage requirements. Long-term or permanent value records can be identified by checking the Retention and Disposal Authority and/or by requesting advice through an Information and Data Management Assessment.

2.4. The capture, collection or creation of information must occur in a manner that appropriately considers the current and future requirements of Monash's operations. For instance, records and other information assets with long-term or permanent value must be archived in a timely manner, in a sustainable format that ensures long-term accessibility and readability.

2.5. Staff must follow all relevant procedures including the Data Privacy and Protection Procedure, Data Privacy and Protection Schedule Monash University Indonesia, Cyber Security Controls, and cyber security standards including the Information Classification and Handling Standard when capturing and managing data, information and records. Adhering to these procedures, controls, and standards helps to ensure appropriate protections are in place for the vast range of information assets within Monash, and will assist Monash to comply with regulatory requirements.

Storage of information

2.6. All information must be stored in Monash's prescribed systems and infrastructure, and be classified according to the Information Classification and Handling Standard.

2.7. Staff or authorised persons must not store Monash information assets on personal or unauthorised devices, such as USB drives, external hard drives, or personal cloud services. Monash information assets must be stored in a manner that ensures they are available for all relevant business needs throughout the asset's full lifespan.

2.8. Information must be preserved securely for the minimum period required under any relevant legislation and subsequently disposed of, or as otherwise directed by Group Information and Records Management.

2.9. When leaving Monash, staff must ensure any relevant documents and information stored in Monash IT environments including, but not limited to, documents, file shares and collaborative environments, have been transferred to the responsibility of the appropriate supervisor. All duplicate, obsolete and non-essential documents should be destroyed following the Normal Administrative Practice processes.

Access to information

2.10. Access to records must be available to authorised personnel to enable prescribed activities for Monash to occur and information to be shared between relevant organisational units.

2.11. Access to all storage systems and information assets contained within them must be limited to individuals with approved access and permissions within the Monash IT environment.

2.12. Access to Monash information assets 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.

2.13. Any person wishing to request access to a document under the Freedom of Information Act 1982 (Vic) may make a request 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.

2.13.1. If, following the receipt of an individual's personal information, the individual finds the information is incomplete, incorrect, out of date or misleading, the individual may ask for the amendment or annotation of the information in accordance with section 5 of the Data Protection and Privacy Procedure and the Data Protection and Privacy Schedule - Monash University Indonesia.

2.14. Staff must immediately notify Monash's Freedom of Information Officer of any requests they receive for access to Monash records and must provide the Freedom of Information Officer with immediate access to all documents that may be relevant to a Freedom of Information Request.

2.15. All staff can request access to archival records 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.

2.15.1. Group Information and Records Management must consult with relevant areas if a request to access archives covers records that may:

- be commercially sensitive, commercial-in-confidence (to Monash or third parties), or contain legal advice;
- contain personal data or sensitive information;
- be subject to confidentiality restrictions including embargoes and/or confidentiality requirements set by University Council and associated committees;
- jeopardise future investigatory functions or law enforcement, or threaten the safety of any person and/or could compromise Monash security if disclosed, such as data centres, chemicals etc; and/or
- contain culturally-sensitive Indigenous information.

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

2.15.3. 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.

Retention and disposal of information

2.16. Records must not be disposed of before the expiration of any minimum retention period even when the information is no longer required for the purpose for which it was captured, collected or created. Staff can seek detailed information on retention and disposal and on the authorisation of records destruction via Monash's Retention and Disposal Authority and local legislative requirements for international locations (if they require longer retention periods than the Monash Retention and Disposal Authority).

2.17. Prior to any destruction of records, managers must confirm that the records are no longer required for legal, administrative, audit or financial reasons. For instance, records must not be destroyed if destruction would breach any legislative requirements, court orders, or if they are likely to be relevant to actual or anticipated legal proceedings or related to a Freedom of Information request.

2.18. Data, information and records can be stored beyond the expiry of the retention period with written approval from the Monash University Australia Director, Information and Records Management confirming that an exemption to support operational requirements has been granted to allow the minimum retention period as outlined in the Retention and Disposal Authority to be extended. Requests for exemptions can be requested by contacting the University Archives.

2.19. For hybrid records containing both paper and digital components, all parts should be disposed of at the same time to ensure consistency and compliance with retention requirements.

2.20. Where migration of records is required, staff must first consider all security, retention and disposal requirements such as the period that records need to be kept and whether they are considered to be of permanent value.

2.21. When disposal of records has been approved, including when a Notice to Delete has been issued, disposal must be implemented securely and completely, with methods appropriate to the level of sensitivity of the information. The disposal of hard copy records may require the use of a confidential waste bin or shredder. The disposal of digital information assets may include ensuring all copies of the data have been appropriately deleted (including backups) at the same time, or shortly afterwards (within 30 days).

2.22. Detailed documentation of all records destroyed must be maintained, including descriptions of records, date ranges, destruction dates, and authorisation. Advice on how to manage such documentation can be obtained via request through submitting an Information and Data Management Assessment.

3. Artificial intelligence systems

3.1. Monash will ensure appropriate recording, retention and storage of Artificial intelligence (AI)-assisted decisions, maintaining accountability, metadata transparency, and compliance with the Information Management Policy and Artificial Intelligence Operations Policy.

3.2. Monash will be transparent and accountable regarding ownership and responsibility in relation to all types of AI used, including undertaking recordkeeping that:

3.2.1. provides a clear acknowledgement of text, images, sound or video produced by generative AI;

3.2.2. documents appropriate oversight and responsibility for each AI system used, including obligations related to timely disposal activities and recording events such as AI system failures, and malicious use; and

3.2.3. safeguards information integrity and demonstrates an understanding of the legal requirements or obligations applicable to each system.

4. Roles and Responsibilities

4.1. Monash is responsible for all information, data and records within its information assets and its existing governance structure will provide high-level governance for information management.

4.2. All staff and associates are responsible for being ethical, transparent, proactive, accountable and cooperative in creating and managing Monash records and information. This includes:

4.2.1. compliance with policies, procedures and schedules related to information management, and safeguarding personal data against unauthorised access, loss, misuse, modification, or disclosure, such as the Data Protection and Privacy Procedure and the Data Protection and Privacy Schedule Monash University Indonesia;

4.2.2. understanding what information and records are required to be created, captured and maintained for their role within Monash;

4.2.3. ensuring that Monash information assets are maintained in ways that enables them to be relied upon consistently as complete, secure and authentic sources of information;

4.2.4. ensuring information assets are able to support accurate recordkeeping when required; i.e. the information assets can provide evidence of Monash decisions and actions in a way that supports the transparency and accountability requirements of the institution; and

4.2.5. following any locally issued information governance and recordkeeping processes, standards and/or guidelines.

4.3. All staff with OHS recordkeeping responsibilities must:

4.3.1. follow relevant sentencing requirements for OHS records, as outlined in the OHS section of the Retention and Disposal Authority; and

4.3.2. adhere to the approved destruction processes as outlined by the University Archives in the Retention and Disposal Authority.

4.4. Monash will provide relevant staff with guidance and training for effective recordkeeping and information management practices to foster a culture of responsible recordkeeping and information management, and ensure staff are equipped with the necessary knowledge to manage records effectively and in compliance with legal requirements.

Information Governor

4.5. Information Governors are accountable for ensuring that information assets (including any nominated Monash IT environment, software and platforms) are managed appropriately under their governorship, and are tasked with the following responsibilities:

4.5.1. ensuring information assets are able to comply with all relevant Monash policies, procedures and schedules as well as any related legislative requirements. This includes ensuring that Monash information is not stored in environments (including cloud environments) that are not capable of complying with relevant legislation and policy directives.

4.5.2. accountability for the quality and integrity of the data in the information asset, as well as having responsibility for ensuring all relevant assessments for the information assets are completed and up to date; specifically the Information Security Risk Assessments, Privacy Impact Assessments, and Information and Data Management Assessment. This includes identifying outdated information assets that contain obsolete, trivial or redundant information, or may be performing technically poorly (e.g. no longer within a technical support agreement), and reviewing the above assessments when upgrading, migrating and/or decommissioning systems.

4.5.3. understanding the data held within each information asset and for ensuring that the most appropriate metadata and classification structures (including data definitions) are in place and being adhered to. This will ensure that the data can be identified, located and used for the entirety of the information asset's lifespan.

4.5.4. ensuring information assets do not contain unnecessary duplicate data.

4.5.5. acknowledging that the information asset will be registered in the Information Asset Register and accountable for updating the catalogue on request.

4.5.6. ensuring permanent value records, as identified in the Retention and Disposal Authority, have their capture and management requirements (including future preservation needs) negotiated in consultation with the University Archives as soon as they are identified. In certain cases this process may involve transferring custody of these assets to the University Archives, where appropriate and practical.

4.5.7. where any kind of transfer or migration is required, ensuring that information assets, particularly the Monash IT environment, have

a documented export solution available from vendors for both on premise and Software as a Service arrangements. This is to ensure Monash retains full responsibility and control of data, information and records for the entirety of the information asset's lifespan.

4.5.8. ensuring any information management directives and Notice to Delete instructions are implemented within a reasonable timeframe.

4.5.9. authorising and managing access to information assets based on the relevance of job functions, roles, and responsibilities, while maintaining appropriate documentation and adhering to Monash policies, procedures and schedules.

Information Steward

4.6. Each information asset (most likely to take the form of Monash systems such as Callista, TRIM) may have one or more Information Stewards appointed by the relevant Information Governor depending on the complexity of the information asset.

4.7. Information Stewards must understand relevant Monash policies and procedures as well as any related legislative requirements that could impact the management of the information asset.

4.8. Information Stewards are responsible for ensuring compliance with all information management processes, including any set out in the Information Security Risk Assessments, Privacy Impact Assessments, and Information and Data Management Assessment.

4.9. Information Stewards are responsible on behalf of the Information Governor to implement and ensure compliance with comprehensive data management processes throughout the data lifespan, ensuring the quality of the information in the Monash IT environment 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 system are maintained and preserved for the lifespan of the asset.

Group Information and Records Management

4.10. Group Information and Records Management is responsible for establishing and managing the operational processes to support the Information Management Policy and this procedure.

4.11. Group Information and Records Management is responsible for providing direction and coordination of central information management responsibilities such as the Information and Data Management Assessments, developing and maintaining the Retention and Disposal Authority, authorising Notices to Delete, overseeing archives collections and management processes, approving access requests to the University Archive collections, and preservation of the physical and digital University Archives.

4.12. Group Information and Records Management will establish and maintain the Information Management Framework to guide the implementation of the procedures outlined in this document.

DEFINITIONS

Artificial Intelligence (AI) Systems	Innovative advancements encompassing AI technologies used in computer software, programs, applications and tools, including Generative Artificial Intelligence (GenAI).
Associates	For the purposes of this procedure, 'associates' are defined as contractors, conjoint appointments, affiliates and adjunct appointees.
Data	Data are measurements and observations, including facts, figures, records, statistics or opinions, whether true or not, that have been collected directly or obtained as a by-product of a compliance, regulatory or service-delivery process. Data includes information about persons, businesses and other organisations and their characteristics, practices and activities.
File-hosting services	File hosting is an online service that allows users to upload, store, and share files over the internet, providing access and management across multiple devices.
Generative Artificial Intelligence (GenAI)	Artificial Intelligence that possesses the ability to autonomously create or generate new content, data, or information, often based on learned patterns and examples from existing datasets and using transformer or diffusion AI models. Further information on Monash's use of AI can be found at AI at Monash website and Teach HQ.
Information	Consists of data that has been processed, analysed, or interpreted within a given context. Information can exist in any format. Examples include physical (paper) or digital (audio, PDF file, .jpeg).

Information asset	An information asset is a body of information, defined and practically managed so it can be understood, shared, protected and used to its full potential. Monash's Information Asset Register provides details about the assets and the information contained within them.
Monash IT environment	For the purposes of this procedure, 'Monash IT environments' includes all IT infrastructure including electronic devices, hardware, software, networks, websites, systems and services owned or controlled by Monash, or a Monash controlled or associated entity.
Normal Administrative Practice (NAP)	A process that allows Monash to destroy certain types of low-value and short-term information in the normal course of business. Refer to the NAP process for further information.
Permanent value record	A record defined as permanent in the Records Retention and Disposal Authority, because it has been appraised to have ongoing historical and/or cultural value.
Public records	Data, information, and records are all public records that require management in accordance with the Public Records Act 1973 (Vic).
Record	Information in any format created, received, and maintained as evidenced by Monash, in pursuant of legal obligations or in the transaction of business.
Recordkeeping	An all encompassing description of activities relevant to the record lifespan (i.e. length of time it is in existence). Encompasses the decision to create records, their management throughout the multiple contexts of creation and use, and their preservation or destruction based on ongoing needs.
Retention period	The minimum period that records must be kept before they can be legally destroyed.
Sentencing	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.

GOVERNANCE

Parent policy	Information Management Policy
Supporting procedures	Data Protection and Privacy Procedure
Supporting schedules	Data Protection and Privacy Schedule Monash University Indonesia
Associated procedures	Artificial Intelligence Operations Procedure Information Security and Classification Management Procedure Research Data Management: Graduate Research Student Procedures Research Data Management: Staff, Adjuncts and Visitors Procedures
Related legislation	***Australia*** Evidence Act 2008 (Vic) Freedom of Information Act 1982 (Vic) Public Records Act 1973 (Vic) Health Records Act 2001 (Vic) Privacy and Data Protection Act 2014 (Vic) Privacy Act 1988 (Commonwealth) Public Records Act 1973 (Vic) ***China*** Data Security Law Personal Information Protection Law Cybersecurity Law ***Europe/Italy*** General Data Protection Regulation (GDPR)

	Legislative Decree No. 196/2003 ***Indonesia*** Law No. 11 of 2008 regarding Electronic Information and Transactions, as amended by Law No. 19 of 2016 ("Electronic Information Law") Law No. 27 of 2022 on Personal Data Protection Government Regulation No. 71 of 2019 regarding the Implementation of Electronic Systems and Transactions ("GR 71") Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data ("MOCI Reg. 20") ***Malaysia*** Companies Act 2016 Employment Act 1955 Income Tax Act 1967 Official Secrets Act 1972 Personal Data Protection Act 2010 Private Higher Educational Institutions Act 1996 Sales Tax Act 2018 Service Tax Act 2018
Category	Operational
Approval	Chief Operating Officer 29 April 2025
Endorsement	Executive Director, eSolutions 28 April 2025
Procedure owner	Director, Information and Records Management
Status	Current and in effect
Date effective	5 May 2025
Version	1.0
Content enquiries	groupinformationmanagement@monash.edu