INFORMATION MANAGEMENT POLICY

SCOPE

This policy applies to all staff, students, associates and visitors who handle information assets at Monash. For research data management, staff, students and associates must refer to the Research Data Management Policy.

For the purpose of this policy, references to 'Monash' include Monash University Australia, Monash University Malaysia, Monash University Indonesia, Monash College, Monash Investment Holdings, Monash Suzhou, the Monash University Prato Centre, and the World Mosquito Program Ltd (and its subsidiaries), unless indicated otherwise.

This policy will operate in jurisdictions outside 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 Australia; a reference below to 'law' is a reference to the law governing that campus or those operations.

POLICY STATEMENT

Information management encompasses the collection, access, use, storage, retention, governance, disclosure and disposal of information assets (records, information and data) in any format, created or received, to support Monash activities. This includes information managed across all information technology (IT) systems, software, and platforms including databases, email, voice and instant messaging, images, videos, websites, and social media applications. It also covers information created and managed in-house and offsite, including in cloud-based platforms or unmanaged systems outside Monash IT environments.

Monash is committed to the responsible, ethical and effective management of its information assets to support its education, research and operational activities globally. The management of these assets must comply with this policy and related policies, including the Cyber Security Management Policy, Research Data Management Policy and Artificial Intelligence Operations Policy, to ensure the integrity, governance, security and availability of information assets across all Monash locations.

Information must be managed in a way that promotes transparency, security, data protection, and privacy, ensuring compliance with regulatory and contractual obligations and ethical standards.

1. General principles

1.1. Monash is committed to managing its information assets ethically, recognising that many of those assets contain information about individuals whose trust and dignity are prioritised. Monash is also committed to ensuring compliance with all applicable regulatory, contractual, and policy requirements governing the collection, access, use, storage, retention, disclosure, transfer, and disposal of information assets.

1.2. Monash will only collect and process personal data, sensitive information and health information that is necessary to fulfil its functions and activities, and in compliance with applicable privacy laws. The Data Protection and Privacy Procedure, Data Protection and Privacy Schedule - Monash University Indonesia, Monash University Malaysia's Personal Data Protection Notice and Data Protection and Privacy Collection Statements outline what personal data is processed by Monash, the purposes for which it is used, disclosed and otherwise processed, and how individuals can exercise their rights in relation to the personal data Monash holds about them.

1.3. The identification and management of information, data and recordkeeping risk is the responsibility of all staff, and requires a concerted effort across all Monash operations.

1.4. Over- or under-retention of information assets poses a significant risk to Monash. Monash staff must follow the retention period for information assets, as set out in the Retention and Disposal Authority. Information assets will be retained only as long as necessary and disposed of securely to minimise risk to Monash and individuals.

1.5. Monash will classify information assets in line with the Information Security and Classification Management Procedure and the Information Classification and Handling standard.

1.6. Monash recognises that maintaining trust and confidence in the management and protection of information assets is essential to its operations and reputation, and it is committed to creating and keeping accurate, reliable and secure records in order to:

- support efficient and effective operations, ensure accountability and regulatory compliance; and
- preserve institutional memory, which captures Monash's collective knowledge, informs decision-making, and ensures continuity in governance, teaching, and research.

1.7. Monash will use relevant information management controls and processes in order to:

- safeguard and secure the confidentiality, integrity and availability of its information assets;
- facilitate a culture where Monash information assets are trusted and well-described;
- store information assets in known, endorsed locations for their applicable lifespan; and
- ensure that information assets are able to be identified, retrieved and used for the period of time they must be retained.

1.8. Monash is responsible for all information, data, and records within its information assets. The leadership and oversight of information management are guided by this policy and the Information Governance and Recordkeeping Procedure and supported by relevant governance groups to ensure effective protection and management of information assets throughout their lifespan.

1.9. Monash recognises the increasing role of Artificial Intelligence (AI) in information creation and processing. This policy requires that AI-generated or processed information is handled in alignment with Monash's Responsible Use of AI Principles that apply to both students and staff across the Monash Group, as outlined in the Artificial Intelligence Operations Policy.

1.10. Monash is committed to the ethical collection and management of personal data including how it is shared and accessed over time. Monash will consult the Deputy Vice-Chancellor (Indigenous) in relation to management of data pertaining to Indigenous peoples (other than ordinary staff or student records).

2. Managing information across its lifespan

2.1. Monash recognises that its information assets have varied and sometimes competing values, which can present differing risks across the information asset lifespan. As such, information assets:

2.1.1. must be managed to ensure that they inform improvements in Monash's operations;

2.1.2. must be managed in a way that enables them to be accessible for the purposes of administering requests for access, including Freedom of Information requests, requests for production of documents (including as part of legal proceedings), and for activities such as audits and internal investigations;

2.1.3. require protection against unauthorised access, use, modification or disclosure, with additional protection given to information assets containing personal data and sensitive information; and

2.1.4. must be disposed of when there is no longer any operational need or legal requirement to retain them. Information assets are to be retained beyond the prescribed retention periods in the Retention and Disposal Authority only after review and approval by Group Information and Records Management. Some information assets will form part of Monash's institutional memory and will require management and preservation by the University Archives to ensure the asset(s) is permanently accessible and fit for use.

2.2. Information, data and records must be maintained within Monash IT environments that are capable of meeting all relevant information and recordkeeping legislative requirements, standards, procedures and controls across the asset's lifespan.

2.2.1. Monash information assets should not contain unnecessary personal data, nor hold onto personal data longer than the minimum retention period, as set out in the Retention and Disposal Authority unless there is a legal or approved (by Group Information and Records Management) operational requirement to do so.

2.2.2. Monash will ensure that it is collecting accurate and reliable data from trusted sources, including directly from individuals for personal data, where reasonably practicable.

2.2.3. Monash will take an active role in reducing the amount of unnecessary duplication of data and information it collects and manages within its information assets.

2.2.4. Information, data and records must be stored in conditions suitable to the information asset's lifespan and the nature of the content, and must comply with the Information Security and Classification Management Procedure.

2.3. The University Archives will maintain a Group-wide Retention and Disposal Authority specifying the required retention periods for information assets based on regulatory and operational requirements. These retention schedules will be periodically reviewed by University Archives and based on assessment, analysis and strategic mitigation of risk to Monash.

2.4. All Monash information, data and records must be retained and disposed of in accordance with the Retention and Disposal Authority or Normal Administrative Practice.

3. Information access, sharing and security

Access and sharing

3.1. Information, data and records must be made available to support the operations of Monash and as stipulated in legislation and within the constraints of security, confidentiality, privacy, data protection, and relevant recordkeeping guidelines across their lifespan.

3.1.1. Access to information assets from within and across Monash shall be based on the job function, role and responsibilities of the individuals requiring access to the asset to perform their official duties.

3.1.2. Monash will ensure that the information asset is readily discoverable, provided in the right format, and in a timely manner in order to support Monash's operational requirements.

3.1.3. Access to information assets in the custody of the University Archives for research by external parties and by Monash staff for research purposes not directly related to their job function, role or responsibilities will be made available in accordance with clause 2.15 of the Information Governance and Recordkeeping Procedure and subject to privacy obligations if personal data is involved.

Freedom of information requests - Monash University Australia

3.2. Monash is committed to transparency and providing access to information where required by law. A request for access to documents held by Monash can be made by any person under the Freedom of Information Act 1982 (Vic) and should be made in accordance with clause 2.13 of the Information Governance and Recordkeeping Procedure.

Information security

3.3. All information assets must be securely stored in authorised locations, with appropriate safeguards, such as encrypted storage devices, secure servers or cloud-based storage approved by the Portfolio of the Chief Operating Officer, to protect against unauthorised access, loss or damage throughout their lifespan.

3.4. Information assets are classified based on their confidentiality, integrity and availability with appropriate security controls applied in accordance with the Information Security and Classification Management Procedure.

3.5. If orphaned (or unclaimed) data or information assets are discovered, the matter will be referred to Group Information and Records Management who will take the necessary action to bring the data under appropriate management and ensure it is compliant with this policy.

4. Risk mitigation and management

4.1. Monash employs a risk-focused approach to its information management strategy that is aligned with the Group Risk Management and Compliance Policy, and leverages the following key principles to ensure a robust and adaptive strategy that effectively mitigates potential vulnerabilities while maximising the value of information assets. The principles of this strategy include:

- consistency in information management and retention practices across Monash to mitigate the risk of breaches;
- clear responsibilities and custodianship for managing and securing information assets;
- reliability and integrity of information, data and records to ensure they are complete, consistent, accessible, not unnecessarily duplicated, and reliably support and substantiate Monash decision-making; and
- safe storage, retention and disposal of data and information that uses current technologies, and is protected against theft and accidental loss.

4.2. Monash employs a range of authorities, frameworks, controls, and tools to identify and manage risks associated with information assets. Amongst these are the Cyber Security Management Policy, Information Security and Classification Management Procedure, Data Protection and Privacy Collection Statements, Retention and Disposal Authority, and the Information Asset Register.

5. Breach of Policy

5.1. Monash treats any breach of its policies, procedures and schedules seriously; it encourages reporting of concerns about non-compliance, and manages compliance in accordance with the applicable Enterprise Agreement, relevant instrument of appointment and/or applicable contract terms. A failure to comply with this policy and its supporting procedure(s) may result in action by Monash. Such action may include disciplinary and other action up to and including potential termination of employment, or for associates and other persons, the termination of engagements with Monash.

DEFINITIONS

Associates	For the purposes of this policy, '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.
Disposal	A range of processes associated with implementing records retention, destruction, or transfer decisions, which are documented in the Retention and Disposal Authority.
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.
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.
Orphaned data	Data with no clear line of ownership.
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.

GOVERNANCE

Supporting procedures	Information Governance and Recordkeeping Procedure Data Protection and Privacy Procedure
Supporting schedules	Data Protection & Privacy Schedule - Monash University Indonesia
Associated policies	Artificial Intelligence Operations Policy Cyber Security Management Policy Group Risk Management and Compliance Policy Research Data Management Policy
Related legislation	***Australia*** Higher Education Standards Framework (Threshold Standards) 2021 (Commonwealth) Higher Education Support Act 2003 (Commonwealth) Health Records Act 2001 (Vic) Privacy and Data Protection Act 2014 (Vic) Privacy Act 1988 (Commonwealth) Public Records Act 1973 (Vic) Freedom of Information Act 1982 (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*** The Computer Crimes Act 1997 Personal Data Protection Act 2010 Private Higher Educational Institutions Act 1996
Category	Operational
Approval	Vice-Chancellor 29 April 2025
Endorsement	Chief Operating Officer 29 April 2025
Policy owner	Director, Information and Records Management
Status	Current and in effect
Date effective	5 May 2025
Version	1.0
Content enquiries	groupinformationmanagement@monash.edu