

# DATA PROTECTION AND PRIVACY PROCEDURE

## SCOPE

This procedure applies to all Monash staff, students and associates and any individual whose personal data is collected for Monash-related purposes, including but not limited to education, research and operational activities.

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

Staff and students at Monash University Indonesia should refer to the [Data Protection and Privacy Schedule - Monash University Indonesia](#).

This procedure applies to staff, students and associates 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 of Australia, a reference below to 'law' is a reference to the law that applies to that campus or those operations.

## PROCEDURE STATEMENT

Monash is committed to respecting and protecting the privacy of every individual and to processing personal data responsibly and transparently, and in compliance with all applicable legal requirements. Together with the [Data Protection and Privacy Collection Statements](#), this procedure explains what personal data is processed, the reasons it is needed to be processed and used, who Monash shares personal data with and how individuals can exercise their rights regarding the personal data Monash holds about them.

### 1. Collecting and processing personal data

- 1.1. Monash will only collect and process personal data to the extent necessary to fulfil Monash's functions and activities, and where there is a lawful basis for doing so.
- 1.2. Personal data collected and held by Monash is processed in accordance with the [Data Protection and Privacy Collection Statements](#) ('Collection Statements') applicable to an individual's relationship with Monash. Depending on this relationship multiple Collection Statements may apply to the same individual, for example as a prospective student, employee, alumni, or based on specific location.
- 1.3. If any of Monash's personal data processing activities fall outside the scope of this procedure or the relevant Collection Statement, Monash will provide individuals with additional information about the processing of their personal data at the time of collection. Monash will only process sensitive or health information with an individual's consent or where otherwise permitted by law.
- 1.4. Monash will, where practicable, collect personal data directly from individuals. Collection Statements outline the instances where Monash may process personal data obtained indirectly from a third party.
- 1.5. Any automated decision-making processes, including profiling, will be set out in the relevant Collection Statement(s) or specifically notified to individuals at the time of engaging with them and will be subject to applicable laws and the Responsible Use of Artificial Intelligence principles outlined in the [Artificial Intelligence Operations Policy](#).

### 2. Automatic data processing

- 2.1. Some types of personal data may be collected automatically by Monash when individuals use Monash websites, mobile applications, Wi-Fi networks, or other Monash IT environments. Additionally, location data within Monash premises, captured through Wi-Fi or mobile applications, and personal data or images obtained from video surveillance and lecture recording systems may also be collected by Monash.
- 2.2. Monash websites use cookies and related technologies to deliver content specific to individual preferences, support authentication and to enhance security. Further information about the use of cookies, including options to disable certain cookies, is available on the [Terms and Conditions](#) webpage.

### 3. Use and disclosure of personal data

- 3.1. Personal data collected by Monash is used to support its education, research and operational activities, including:
- administering student enrolments and the employment of staff;
  - assisting prospective and current students and staff in their academic and professional activities;
  - conducting analytics, such as monitoring traffic flows, to optimise space utilisation and campus management;
  - authorising and securing Monash IT environments, including monitoring unauthorised access and ensuring system availability in accordance with the [Cyber Security Management Policy](#);
  - managing the security and safety of Monash premises to protect students, staff and visitors;
  - fulfilling public health obligations and providing necessary emergency or safety communications;
  - conducting and administering clinical trials and other research activities;
  - sending communications, including marketing communications (as permitted by law);
  - addressing inquiries, requests and other administrative functions; and/or
  - executing specific purposes as outlined in the relevant Collection Statement(s) associated with an individual's interaction with Monash.
- 3.2. Personal data may be disclosed to third parties to the extent necessary for:
- engaging with legal advisers and consultants;
  - when permitted or required by law, such as engaging with law enforcement or regulatory authorities, or in circumstances involving a serious threat to life, health or safety;
  - sharing data with external contracted service providers, such as IT infrastructure and service providers, insurers, auditors or third-party payment processors, to facilitate Monash operations and validate services; and
  - sharing data with affiliated institutions, such as Monash subsidiaries or research partners, to support collaborative research, education, and community engagement initiatives.
- 3.3. Monash assigns employees and students with a unique identifier in the form of a staff or student ID number. Staff and student ID numbers are personal data and will be handled in accordance with this procedure and the law. Except to the extent permitted by the law, Monash will not use government identifiers (such as tax file numbers, Medicare numbers etc.) as identifiers, nor will Monash disclose such identifiers.
- 3.4. Monash will provide individuals with the option to remain anonymous or use a pseudonym where it is lawful and practicable. However, in most cases, it will not be possible to engage with students or staff without proper identification or through the use of a pseudonym.
- 3.5. A [Privacy Impact Assessment \('PIA'\)](#) must be undertaken when introducing or modifying a Monash enterprise or research project, system or process that involves the processing, use, disclosure or storage of personal data. The PIA identifies privacy compliance risks and provides recommendations regarding these risks.

### 4. Security and quality of personal data

- 4.1. Monash is committed to maintaining the integrity and safeguarding of personal data. Reasonable steps will be taken to ensure that appropriate technical and operational measures are implemented so that personal data processed, stored, used or disclosed is:
- accurate, complete and up to date;
  - protected from misuse, loss, unauthorised access, modification or disclosure; and
  - managed in accordance with the [Information Governance and Recordkeeping Procedure](#) and the [Cyber Security Management Policy](#).
- 4.2. Monash will endeavour to ensure that contracted service providers are subject to a law, binding scheme or contract that provides similar protection of the personal data as provided for by applicable privacy laws.
- 4.3. The [Artificial Intelligence Operations Policy](#) and [Artificial Intelligence Operations Procedure](#) apply to the processing of personal data processed and generated by Artificial Intelligence (AI) systems. Staff must comply with this procedure when using AI systems, including undertaking a PIA and/or Information Security Risk Assessment (ISRA) where necessary.

### 5. Access and correction of personal data

- 5.1. Individuals have rights to request access to, or correction of their personal data held by Monash.
- 5.2. Table 1 sets out the appointed Monash primary contacts to request access to or correction of personal data.

**Table 1 - Monash primary contacts to request access to or correction of personal data**

Location	Individuals
Monash University Australia, Monash University Prato Centre, Monash Suzhou	<ul style="list-style-type: none"><li>• Students - <a href="#">Monash Connect</a></li><li>• Staff - <a href="#">Monash HR</a></li></ul>

	<ul style="list-style-type: none"> <li>Alumni, friends and supporters - <a href="#">Alumni Connect</a>.</li> <li>All other queries can be directed to the <a href="#">Data Protection and Privacy Officer</a>.</li> </ul>
<b>Monash University Malaysia</b>	Individuals should direct requests to the Monash University Malaysia Privacy Officer at <a href="mailto:mum.privacy@monash.edu">mum.privacy@monash.edu</a> .
<b>Monash College</b>	Individuals should direct requests to the Monash College Privacy Officer at <a href="mailto:privacy@monashcollege.edu.au">privacy@monashcollege.edu.au</a> .
<b>World Mosquito Program</b>	Individuals should direct requests to the World Mosquito Program Privacy Officer at <a href="mailto:privacy@worldmosquito.org">privacy@worldmosquito.org</a> .

- 5.3. Additional rights may be available to individuals, including those outlined in the Collection Statements depending on the nature of their interaction with Monash.

## 6. Transfer of personal data

- 6.1. Monash may transfer personal data outside of the jurisdiction in which it was collected when necessary to support its operations or to facilitate activities conducted by individuals through or on behalf of Monash. For example, this may occur when a student is studying or a staff member is working at an international location, or when Monash engages the services of contracted service providers.
- 6.2. Where Monash transfers personal data between jurisdictions, it will take all reasonable steps to protect the personal data being transferred. Such reasonable steps may include:
- de-identifying personal data;
  - determining if the recipient is subject to a legal or binding scheme that provides protection which is substantially similar to the applicable privacy laws;
  - contractual arrangements requiring the recipients of the personal data to handle information in accordance with the applicable laws;
  - seeking the consent of the individual prior to transferring the personal data; and/or
  - as is otherwise permitted or required by law.

## 7. Privacy framework

- 7.1. Monash maintains a global privacy framework aligned with the [Group Risk Management Framework](#) (staff login required), ensuring compliance with applicable privacy laws across the Monash Group. To ensure compliance with applicable privacy laws, each entity within the Monash Group must designate a local privacy contact.
- 7.1.1. The Global Data Protection Officer is responsible for overseeing the application of the global privacy framework. Data Protection Officers are appointed in jurisdictions where Monash operates, where required by applicable law.
- 7.2. The [Data Protection and Privacy Office](#) is responsible for coordinating and supporting privacy risk management activities across Monash, including:
- the provision of privacy advice and support;
  - management of privacy-related incidents and complaints;
  - developing and publishing documents to support this procedure; and
  - the provision of privacy-related training and education for staff.

## 8. Opting-out of receiving material produced by Monash

- 8.1. Individuals may opt-out of receiving communications from Monash by using the unsubscribe options provided in each communication or by contacting the [Data Protection and Privacy Office](#), specifying the communications they no longer wish to receive.
- 8.1.1. Communications necessary for the effective operation of Monash and the fulfilment of its core functions, particularly those sent to staff and students, are not subject to opt-out.

## 9. Complaints relating to how personal data is handled

- 9.1. If there are concerns that personal data has not been handled in accordance with this procedure, the relevant Collection Statement(s), or otherwise in accordance with applicable laws, a [written complaint](#) may be lodged with the [Data Protection and Privacy Office](#).

- 9.2. If the response to the complaint is unsatisfactory, or if there are ongoing concerns about how personal data is being used, a complaint can be lodged with the appropriate regulatory body. For further details refer to the [Data Protection and Privacy](#) webpage.

## 10. Reporting data and privacy incidents

- 10.1. Any data or privacy incident, including an actual or suspected data breach, must be immediately reported to the [Data Protection and Privacy Office](#).
- 10.2. A data or privacy incident means an actual or suspected data breach as defined under applicable privacy laws, including:
- the use or disclosure of personal data for a purpose that is not authorised by the individual or by law; or
  - the loss, accidental or unlawful destruction, misuse, unauthorised access, alteration or unauthorised disclosure of personal data.

## DEFINITIONS

Artificial Intelligence (AI)	The science and technology of creating machines or systems that can perform tasks that normally require human intelligence, such as understanding language, recognising images, or assisting in decision-making in line with Monash's Principles for the Responsible Use of Artificial Intelligence.
Artificial Intelligence (AI) Systems	Innovative advancements encompassing AI technologies used in computer software, programs, applications and tools, including Generative Artificial Intelligence (GenAI).
Monash IT environment	For the purpose 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.
Personal data	Personal data includes a broad range of information that could identify an individual. For example, an individual's name, signature, address, phone number or date of birth, credit information, employee record information, photographs, internet protocol (IP) addresses, etc.
Sensitive data	Sensitive data is a subset of personal data that may require additional protection under relevant privacy laws. Depending on the jurisdiction, this may include data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, genetic and biometric data, sexual orientation, and criminal record data. Handling of sensitive data is subject to specific legal and regulatory requirements, which may vary by jurisdiction.

## GOVERNANCE

Parent policy	<a href="#">Information Management Policy</a>
Supporting procedures	<a href="#">Information Governance and Recordkeeping Procedure</a>
Supporting schedules	<a href="#">Data Protection and Privacy Schedule - Monash University Indonesia</a>
Associated procedures	<a href="#">Artificial Intelligence Operations Procedure</a>
Related legislation	<p><b>Australia</b></p> <p>Health Records Act 2001 (Vic)</p> <p>Higher Education Standards Framework (Threshold Standards) 2021 (Cth)</p> <p>Privacy Act 1988 (Cth)</p> <p>Privacy and Data Protection Act 2014 (Vic)</p> <p>Public Health and Wellbeing Act 2008 (Vic)</p> <p><b>China</b></p> <p>Data Security Law 2021 (China)</p> <p>Personal Information Protection Law 2021 (China)</p> <p>Cybersecurity Law 2017 (China)</p>

	<p><b>Europe/Italy</b>  General Data Protection Regulation (EU) 2016/679  e-Privacy Directive 2002/58/EC  Legislative Decree No. 196/2003</p> <p><b>Malaysia</b>  Personal Data Protection Act 2010 (Malaysia)  Private Higher Educational Institutions Act, 1996 (amended 2009) (Malaysia)</p>
Category	Operational
Approval	Chief Operating Officer 29 April 2025
Endorsement	General Counsel 16 April 2025
Procedure owner	Director, Data Protection and Privacy
Status	Current and in effect
Date effective	5 May 2025
Version	2.0
Content enquiries	<a href="mailto:dataprotectionofficer@monash.edu">dataprotectionofficer@monash.edu</a>