DATA PROTECTION AND PRIVACY PROCEDURE

OVERVIEW

Monash University is a global university with a distinct international focus. The main functions of the University are to:

- provide education and conduct research;
- provide ancillary activities to support students and employees in their study or work at the University;
- remain in contact with alumni, friends and supporters of the University; and
- ensure the ongoing effective operation of the University.

Monash values the privacy of every individual and is committed to the protection of personal data. This Data Protection and Privacy Procedure ('Procedure') outlines how the University ('us', 'our' or 'we'):

- handles personal data including health information (as defined below), in carrying out our main functions;
- complies with applicable privacy laws in processing personal data, including the Privacy and Data Protection Act 2014 (Vic) (which covers the Information Privacy Principles), the Health Records Act 2001 (Vic) (which covers the Health Information Principles), and to the extent it applies to our activities, the Privacy Act 1988 (Cth) and the General Data Protection Regulation ('GDPR') (which gives certain rights to individuals who are based in the European Economic Area (EEA) during their interactions with us or to individuals who interact with the Monash Prato Centre).

This Procedure, together with the Data Protection and Privacy Collection Statements ('Collection Statements') described below, supports the principle of responsible and transparent handling of personal data by explaining what personal data we process, the reasons why we need to process and use it, who we share it with and how you can exercise your rights in relation to the personal data that we hold about you.

The ways in which we process and use your personal data will vary depending on your relationship with us and we rely on a number of legal bases to lawfully process your personal data (see section 1).

SCOPE

This Procedure applies to personal information, sensitive information, health information, personal data and special category data as defined under applicable privacy laws (collectively referred to as 'personal data' throughout this Procedure and the Collection Statements), regardless of how it is processed or stored (or whether it is hardcopy, electronic or by verbal means).

Employees and students studying at Monash University Malaysia should refer to local policies in relation to data protection and privacy. Where this procedure is adopted by Monash College, it should be read in reference to Monash College.

1. Data Protection and Privacy Office

1.1 The University's Data Protection Officer is responsible for data protection and privacy across the University.

1.2 The Data Protection Officer leads the Data Protection and Privacy Office. The Data Protection and Privacy Office:

- provides expert assistance with interpretation and compliance regarding applicable privacy laws and this Procedure;
- manages data management and privacy related queries, incidents and complaints;
- conducts audits of the University's data management practices;
- develops and publishes supporting documents which assist in the application of this Procedure; and
- coordinates privacy related training and education for University employees.

2. Processing of personal data and our lawful bases

2.1 We will only process personal data that is necessary to fulfil the functions and activities of the University as determined by the nature of your interaction with us and where we have a lawful basis to do so. The processing of your personal data will be by fair means and will not be unreasonably intrusive.

2.2 Our Collection Statements provide detailed information relating to the handling of your personal data, including the lawful basis and purposes for which we are processing your personal data, as well as any individual rights that may be available to you. Your personal data may, at any one time, be processed in accordance with multiple Collection Statements depending on the nature of your interaction with us (e.g. if you are an alumni and also an employee of the University). Our Collection Statements outline how your personal data is collected, moved and shared across the University.

2.3 When you are interacting with us during the recruitment and admissions process to become a student of the University, please refer to the Admissions Data Protection and Privacy Collection Statement.

When you are interacting with us as a student of the University, including as a student of Monash Prato or as a student from another institution on exchange at the University, please refer to the Student Data Protection and Privacy Collection Statement.

When you are interacting with as an alumni, friend and/or supporter of the University, please refer to the Alumni, Friends and Supporters Data Protection and Privacy Collection Statement.

When you are interacting with as an employee of the University or applicant, please refer to the Employee Data Protection and Privacy Collection Statement.

When you are interacting with us as a visitor or enquirer to the University, including as a visitor of Monash Prato, please refer to the Visitors and Enquirers Data Protection and Privacy Collection Statement.

When you are interacting with us as a research participant, please refer to the Monash University Research Data Protection and Privacy Collection Statement.

2.4 You will be given further information about the uses of your personal data when you sign up to use specific University services and facilities that we offer to you which are not covered by this Procedure or a relevant Collection Statement, and in certain situations, you may be asked whether you give your consent to us processing certain information about you. Sensitive information and health information (collectively referred to as 'special category data') will only be processed by us with your specific and informed consent or as otherwise permitted or required by law (including pursuant to any government directions, such as the Public Health and Wellbeing Act Vic (2008).

2.5 We will process personal data directly from you wherever possible.

2.6 In some cases we may need to process your personal data indirectly from a third party, such as from the Victorian Tertiary Admissions Centre (VTAC) and other educational institutions if you are applying to become a student of the University, or an employment agency, a former employer, a contractor or a government authority such as Victoria Police if you are an employee applicant. Please refer to our Collection Statements for more detailed information as it applies to your interaction with us.

2.7 Any automated decision making by us, including profiling, will be set out in our Collection Statements.

3. Automatically processed information, including use of cookies

3.1 Personal data may be automatically processed by us when you visit University campus or premises or use our websites, mobile applications, Wi-Fi and other online services. The types of personal data processed may include:

- user names, passwords and other registration details that you provide when registering to use any of our websites, mobile applications or other services;
- details of your visits to, and use of, our websites, mobile applications, Wi-Fi and other online services, including different parts of those services you access during your visits, your IP address, and the date and time of your access;
- where you use our Wi-Fi or mobile applications, your location on our premises as identified by the Wi-Fi or mobile application;
- This may include device details such as device identifiers, usage and location data, and, if you have logged into Monash;
- Eduroam (or other such wireless connections), your username;
- the IP address of your wireless enabled device while you are on our premises as wireless traffic is monitored; and
- when on our premises, personal data and images collected from video camera surveillance.

3.2 The University website uses cookies and related technologies. A cookie is a small message given to your web browser by our web server. The browser stores the message in a text file and the message is then sent back to the server each time the browser requests a page from the server. It is possible to disable the acceptance of cookies by your web browser. However, doing so may restrict your ability to access some web pages. Some University sites are access restricted. These sites may use cookies to deliver content specific to your interest. Cookies may also be used for authentication purposes and to improve security during a visitor's session online. Please refer to our Website Terms and Conditions for more detailed information.

4. Use and disclosure of personal data

4.1 Personal data processed by the University is used and disclosed for the following purposes:

- to support prospective and current students and employees in their study or work with the University;
- to provide analytics, including traffic flows in and around our facilities, for the purpose of space utilisation and campus management functions;
- to ensure the use of the Monash network is authorised, to protect against unauthorised access, to monitor the use and availability of the network, and system administration purposes, facilities and services;
- in the management, security and safety of our premises generally and for the safety and security of University students, employees and visitors;
- to enable the University to meet its public health obligations;
- the provision of emergency or safety messages and to facilitate appropriate assistance in the event of an emergency including to comply with any government directions;
- in the course of addressing enquiries and requests; and
- for the specific purposes outlined in the Collection Statement(s) that apply to your interaction with us.

4.2 Your personal data may be disclosed to the University's legal advisers or other professional advisers and consultants engaged by the University.

4.3 Personal data may be used or disclosed by the University where permitted or required by law. This will usually be where it is necessary to lessen or prevent:

- a serious threat to your life, health, safety or welfare; or
- a serious threat to public health, public safety or public welfare.

4.4 In addition, we may, from time to time be required to disclose your personal data to third parties, such as:

- corporate and public sector organisations to facilitate and enable opportunities for community engagement, work integrated learning activities and student placements;
- off-shore Monash campuses and Monash associated teaching and researching institutions to facilitate and enable opportunities for employee/student research, work and scholarship opportunities;
- law enforcement or other government and regulatory bodies as required by law;
- external third party providers such as our insurers or those who require the information to provide a service to Monash or for the purposes of checking the quality of the services we provide (e.g. our auditors); and

- third party payment processors for the purposes of validation where payments are made online to the University.

4.5 Any other uses or disclosures that the University makes will be where permitted by law or other lawful bases (as notified to you) and your interests will always be considered. Where the University is required to disclose your personal data to third parties, we will always seek to share the minimum amount of personal data necessary.

4.6 Some University sites may have chat rooms, forums, online teaching environments, message boards and/or news groups available to users. Please remember that any information that is disclosed in these areas may become public information and you should exercise caution when deciding to disclose your personal data.

5. Security and quality of personal data

5.1 We are committed to the integrity and safeguarding of personal data and take all reasonable steps to ensure that the personal data we process, maintain, use or disclose is:

- accurate, complete and up to date;
- protected from misuse, loss, unauthorised access, modification or disclosure; and
- managed in accordance with the University's Recordkeeping policy and the Recordkeeping: Retention and Disposal of University Records procedures (Australia only).

5.2 Physical, technical and appropriate protective data security practices are applied to all personal data held by us.

5.3 University sites have security measures in place against the loss, misuse and alteration of information as defined in the University's IT Security Policy.

5.4 When using contracted service providers, we endeavour to ensure 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.

6. Access and correction of personal data

6.1 You should ensure your personal data is accurate, complete and up to date.

6.2 You have a right to access or correct the personal data that we hold about you.

6.3 If you would like to request access to, or correction of, your personal data and you are a student, please contact Monash Connect. If you are an employee, please contact Monash HR. If you are an alumni, friend and/or supporter, please contact External Relations, Development and Alumni.

6.4 If you are not covered by section 6.3 and you would like to request access to, or correction of, your personal data, please contact the Data Protection and Privacy Office.

6.5 The Collection Statements provide further details on the additional rights that may be available to you in certain circumstances depending on the nature of your interaction with us.

7. Use of identifiers

7.1 We will assign employees and students with a unique identifier in the form of a staff or student ID number. Staff and student ID numbers are considered to be personal data and will be handled in accordance with the law.

7.2 Except to the extent permitted by the law, we will not use Commonwealth or State government identifiers (such as tax file numbers, Medicare number etc.) as our own identifiers nor will we disclose such identifiers.

8. Anonymity

8.1 We will provide you with the option of not identifying who you are or using a pseudonym when it is lawful and practicable to do so. However, the nature of the activities conducted by us means that, generally, it is not possible for us to deal with a student or employee anonymously or using a pseudonym.

9. Transfer of your personal data

9.1 Your personal data may be transferred outside of Victoria or outside of Australia where it is necessary for the operation of the University or to facilitate the activities of an individual conducted at or through the University. For example, where a student studies or an employee works at an international campus, or to utilise the services of contracted service providers.

9.2 We may use service providers that are located outside of Victoria and/or Australia and as a result, personal data processed and held by us may be transferred outside of Victoria (but within Australia) or outside Australia.

9.3 Where we transfer personal data outside of Victoria or outside of Australia, we will take all reasonable steps to comply with the relevant Information Privacy Principle relating to trans-border data flows (IPP9). Such reasonable steps may include:

- de-identifying personal data; or
- determining if the recipient is subject to legal or binding scheme that provides protection which is substantially similar to the applicable Information Privacy Principles or Health Privacy Principles; or
- contractual arrangements requiring the recipients of the personal data to handle information in accordance with the Information Privacy Principles and Health Privacy Principles; or
- seeking the consent of the individual prior to transferring the personal data; or
- as is otherwise permitted by law.

9.4 Where we transfer personal data from inside the EEA to outside the EEA, we will, to the extent applicable, comply with the GDPR and take specific measures to safeguard your personal data.

10. Opting out of receiving material produced by the University

10.1 If you do not wish to receive communications from us, you can opt out by utilising the unsubscribe options on the specific publication.

10.2 Alternatively, a written request can be forwarded to the University's Data Protection and Privacy Office at dataprotectionofficer@monash.edu detailing the communications you no longer wish to receive.

10.3 Some University communications to employees and students are not optional and must continue to enable the University to operate effectively and carry out its main functions.

11. Data Protection Impact Assessments

11.1 A Data Protection Impact Assessment ('DPIA') may be undertaken when there is a change to an existing project, system or process, or the introduction of a new project, system or process, that involves a change in current practices for the processing, use, disclosure or storage of personal data. A DPIA is undertaken:

- to ensure legal obligations are met to protect the privacy of any personal data we process, use, disclose, and store;
- to assess the necessity and proportionality of processing in relation to any risks against the rights and freedoms of individuals resulting
- from the processing of personal data;
- to support good governance and informed decision making in the handling of personal data;
- to ensure appropriate risk mitigation considerations to the University, community and individuals in the handling of personal data are considered;
- to assess whether it is safe and appropriate to proceed to the implementation phase of a new activity/project/process; and
- to consider non legal risks related to the planned change such as, but not limited to, individuals being uncomfortable with the use of their information for particular purposes that the University should be sensitive to.

12. Complaints relating to how we handle your personal data

12.1 If you are concerned that your personal data has not been handled in accordance with this Procedure, the relevant Collection Statement(s) and/or your individual rights, you may lodge a written complaint to the University's Data Protection and Privacy Office.

12.2 Your complaint will be appropriately investigated, and the University will provide a response to you, as required, within a reasonable period of time.

12.3 If you are unhappy with the way that we are using your personal data, or if you are not satisfied with our response to a complaint, you may lodge a complaint with the Office of the Victorian Information Commissioner (in relation to personal information and/or sensitive information), the Health Complaints Commissioner (in relation to health information), the Office of the Australian Information Commissioner (to the extent that the Privacy Act 1988 (Cth) applies) or if the GDPR or other jurisdiction's data and privacy law applies, with a Data Protection Authority.

13. Reporting data and privacy incidents and responsibilities

13.1 If you become aware of a data or privacy incident, including an actual or suspected data breach, this must be immediately reported to the University's Data Protection and Privacy Office.

13.2 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.

13.3 Faculties and Divisions are also responsible for appointing a privacy coordinator for the Faculty/Division and informing the University's Data Protection and Privacy Office of changes to any appointment.

13.4 Privacy coordinators are responsible for:

- assisting employees, students and others with general queries regarding data management and privacy;
- escalating queries and data or privacy complaints to the University's Data Protection and Privacy Office where appropriate; and
- informing the University's Data Protection and Privacy Office immediately of data or privacy incidents.

14. Changes to the Procedure and Collection Statements

14.1 We may occasionally make changes to this Procedure and to the Collection Statements from time to time.

14.2 When we make changes, we will make reasonable efforts to bring this to your attention by placing a notice on the website or by sending you an email.

15. Further information and assistance

15.1 If you have any questions, or you would like to find out more about this Procedure and the Collection Statements, please contact the University's Protection and Privacy Office by email dataprotectionofficer@monash.edu

ADMINISTRATION

Parent policy	Integrity and respect
Supporting policies	
Supporting procedures	
Supporting documents	• Monash University Data Protection and Privacy Collection Statements
Legislation mandating compliance	• Privacy and Data Protection Act 2014 (Vic) • Health Records Act 2001 (Vic) • Public Health and Wellbeing Act 2008 (Vic) • Privacy Act 1988 (Cth) • General Data Protection Regulation (EU) 2016/679
Responsibility for implementation	Data Protection and Privacy Office
Approval body	Office of the Chief Operating Officer
Procedure owner	Deputy General Counsel, Office of the General Counsel
Date effective	13 October 2021
Review date	3 years from effective date
Category	Data Protection and Privacy