DATA PROTECTION & PRIVACY SCHEDULE MONASH UNIVERSITY INDONESIA

SCOPE

This Schedule applies to personal data that is collected and/or processed by Monash University Indonesia.

SCHEDULE STATEMENT

Monash University Indonesia ('the University') values the privacy of every individual and is committed to the protection of personal data. This Data Protection and Privacy Schedule ('Schedule') outlines how the University:

- handles personal data (as defined below), in carrying out the University's operations; and,
- complies with all applicable privacy laws in processing personal data.

This Schedule supports the principle of responsible and transparent handling of personal data by outlining the University's commitment and approach to handling personal data in a lawful manner, ensuring the accuracy, completeness, consistency and security of that data. The ways the University processes and/or uses personal data will vary depending on an individual's relationship and/or the nature of the engagement with the University.

1. Lawful bases for the processing of personal data

1.1 The University will only process personal data that is necessary to fulfil the functions and activities of the University, as determined by the nature of an individual's interaction with the University and where there is a lawful basis to do so, for example, teaching and learning and student, and staff administration.

1.2 The University will obtain the consent of the individual concerned for the processing of their personal data for the purposes set out in this Schedule.

1.2.1 The University may ask for additional consent for the processing of certain personal data where current or prospective staff and/or students subscribe for the use of specific University services or facilities not covered by this Schedule.

1.3 When collecting and processing personal data, the University will take reasonable steps to inform the person:

- why the data is being collected and how it is intended to be used;
- the University's authority to collect the information; and,
- any third parties to whom the University routinely gives the kind of data requested.

1.4 Where it is reasonable and practicable to do so, the University will process personal data directly from the individual.

1.4.1 In some case, the University may need to process personal data indirectly from a third party, for example, from a recruitment agency for prospective staff or other educational institutions for prospective students to the University.

Processing personal data of current and prospective students

1.5 Where an individual interacts with the University as a current or prospective student, it will record information as part of the student record. A student record includes:

- details and any applicable supporting documentation provided in an application for admission, including any additional details provided by any referees and anything recorded during or after any interview process.
- information about academic process and standing, exclusion, assessments, results and details of practical and clinical placements (if applicable);
- details such as name, home address, date of birth, course studied, fee payments, financial aid and scholarships; and
- unique personal identifiers assigned to a student (e.g. the student number) and details of any disciplinary or conduct matters.

1.6 The University will indefinitely maintain a student's record following the student's graduation to enable any details of academic achievements to be verified and/or to support historical or statistical research.

1.7 Upon course completion (prior to graduating), a student's contact details will be shared with the External Relations, Development and Alumni Office to be recorded on the University's alumni database. The University provides information on alumni news, events and activities.

Processing personal data of current and prospective staff

1.8 Where an individual interacts with the University as a prospective or current employee, the University will record and/or process the following information:

- details provided directly to the University during any expressions of interest, application, commencement of employment and throughout employment with the University, including any supporting documentation requested or provided, additional details provided by referees or information recorded throughout or after the interview process;
- unique personal identifiers that are assigned to staff (e.g. staff numbers); and,
- details of any disciplinary or conduct issues.

1.9 The personal data that is processed by or on behalf of the University, during any expressions of interest, application, commencement and throughout any employment with the University is collected for the primary purpose of assessing an individual's application for employment, and if successful, administering employment.

1.9.1 Staff who apply for a position through the University's online recruitment service will have their personal data stored on the third-party provider's database.

1.9.2 The University may not be able to consider a prospective staff for employment and/or provide associated services where an individual does not provide their personal data, as requested.

1.10 Current and prospective staff should advise an associated individual if and/or when they are disclosing personal data of that individual to the University, for example, the names and contact details of a referee or emergency contact.

1.11 Should an employment application be successful, the personal data included in the application will become part of a staff member's employment record.

1.11.1 Should an employment application be unsuccessful, the personal data included in the application will be retained for a minimum of five years.

Storage and access to personal data

1.12 All personal data is collected, stored and transmitted securely and in a variety of formats.

1.13 Access to an individual's personal data is limited to the University and University affiliates' representatives who need it for the purpose of carrying out their duties.

2. Automatically processed information, including use of cookies

2.1 Personal data may be automatically processed by the University when visiting the University or using the University's websites, mobile applications, Wi-Fi or other online services. The types of personal data processed may include:

- usernames, passwords and other registration details provided when registering to use any of the University's websites, mobile applications or other services;
- details of visits to, and use of, the University's websites, mobile applications, Wi-Fi and other online services, including different parts of those services accessed during visits, IP address, and the date and time of the access;
- where the University's Wi-Fi or mobile applications are used, or the location on University 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 have logged into Monash Eduroam (or other such wireless connections), the relevant username;
- the IP address of a wireless enabled device while on the University's premises; and
- personal data and images collected from video camera surveillance whilst on University premises.

2.2 The University's s websites use cookies and related technologies. The acceptance of cookies may be disabled but doing so may restrict the ability to access some web pages. Cookies may also be used for authentication purposes and to improve security during a visitor's session online.

3. Use and disclosure of personal data

3.1 Personal data will only be used or disclosed by the University as follows:

- to facilitate and support prospective and current students and staff in their study and/or work with the University;
- to fulfil the University's responsibilities to comply with legislative requirements (including reporting requirements);
- in the course of addressing enquiries and requests;
- to provide analytics for internal and legislative purposes;
- to seek feedback of an individual's experience as a staff or student;
- in the management and security of the University's premises;
- for the provision of emergency and safety messages and to facilitate appropriate assistance in the event of an emergency;

- to legal or professional advisers and/or consultants engaged by the University;
- to offshore collaborative partners;
- to contracted service providers which the University uses to perform services on its behalf;
- to Monash owned entities i.e. Monash University Australia.

3.2 Personal data may also be used or disclosed by the University where required by law. Where the University is required to disclose your personal data to third parties, it will endeavour to share the minimum amount of personal data necessary.

4. Security, protection and quality of personal data

4.1 The University is committed to the integrity and safeguarding of personal data and all reasonable steps will be taken to ensure that the personal data processed, maintained, 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 University's Recordkeeping Policy and applicable legislative requirements.

4.2 Physical, technical and appropriate protective data security practices are applied to all personal data held by the University.

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

4.4 When using contracted service providers, the University will 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.

5. Access to and correction of personal data

5.1 Current and prospective staff and students should ensure that their personal data is accurate, complete and up to date.

5.2 Current and prospective staff and students have a right to access or correct the personal data that the University holds about them.

5.2.1 To request access to, or correction of personal data, staff should contact monashindonesia-recruitment@monash.edu and students should contact Monash Connect.

5.3 Individuals who are not covered by section 5.2 who would like to request access to, or correction of their personal data, please contact mi.enquiries@monash.edu

5.4 Individuals have the right to request deletion of their personal data subject to the minimum retention period and in accordance with the University's Recordkeeping Policy.

6. Use of identifiers

6.1 The University 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.

6.2 Except to the extent permitted by the law, the University will not use government identifiers as its own identifiers, nor will such identifiers be disclosed.

7. Anonymity

7.1 The University will provide the option of not identifying who an individual is or using a pseudonym when it is lawful and practicable to do so. The nature of the activities conducted by the University means that it is normally not possible for the University to deal with a student or employee anonymously or using a pseudonym.

8. Transfer of your personal data

8.1 Personal data may be transferred outside Indonesia where it is necessary for the operation of the University or to facilitate the activities of an individual conducted at or through the University.

8.2 The University may use service providers that are located outside Indonesia and as a result, personal data processed and held by the University may be transferred outside Indonesia.

8.2.1 Where the University transfers personal data outside Indonesia, it will take all reasonable steps to comply with any relevant applicable personal data protection rules in Indonesia.

9. Opting out of receiving material

9.1 The University will enable users to opt out of communications from the University through the unsubscribe options on the specific publication. Alternatively, a written request can be made to mi.enquiries@monash.edu detailing the communications a user no longer wishes to receive.

9.2 Some University communications to staff and students are not optional and are used to enable the University to operate effectively and carry out its main functions.

10. Complaints relating to how personal data is handled

10.1 A written complaint can be lodged at mi.enquiries@monash.edu where an individual is concerned that their personal data has not been handled in accordance with this Schedule and/or their individual rights.

10.2 All complaints will be appropriately investigated and the University will provide a response, as required, within a reasonable period of time.

10.3 If you are unhappy with the way that the University is using your personal data, or if you are not satisfied with the University's response to a complaint, you may lodge a complaint with the Ministry of Communications and Informatics.

11. Reporting data and privacy incidents and responsibilities

11.1 If a student or staff member becomes aware of a data or privacy incident, including an actual or suspected data breach, this must be immediately reported to mi.enquiries@monash.edu.

12. Language

12.1 In compliance with (i) Law of the Republic of Indonesia No. 24 of 2009 dated July 9, 2009 regarding Flag, Language, Coat of Arms and Anthem ("**Law 24**") and (ii) Presidential Regulation of the Republic of Indonesia No. 63 of 2019 dated September 30, 2019 regarding the Use of Indonesian Language ("**PR 63**"), this document is prepared in the Indonesian and English language.

12.2 In the event of any inconsistency between the English language text and the Indonesian language text, or if there should be any dispute on the meaning or interpretation of certain provisions, the Indonesian language text shall prevail and the English language text will be deemed to be amended to conform with and to make the relevant English language text consistent with the relevant Indonesian language text.

DEFINITIONS

Data (or privacy) incident	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.
Minimum retention period	Personal data must be retained for a minimum of five years from when the data is no longer required for the purpose of its collection or processing.
Personal data	Any data about an individual, which may be identified and/or be identifiable jointly and/or individually, either directly or indirectly through electronic and/or non-electronic systems.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

GOVERNANCE

Parent policy	Integrity & Respect Policy
Parent policy owner	Chief Operating Officer
Schedule owner	General Counsel

Associated procedures	Data Protection & Privacy Procedure - Monash University Australia
Legislation mandating compliance	• Government Regulation No. 71 of 2019 (Implementation of Electronic Systems and Transactions); • Minister of Communications and Information Technology Regulation No. 20 of 2016 (Personal Data Protection in Electronic Systems), • Privacy and Data Protection Act 2014 (Vic) (including Information Privacy Principles); • Health Records Act 2001 (Vic) (including Health Information Principles), • Privacy Act 1988 (Australian Cth); • General Data Protection Regulation ('GDPR').
Category	Operational
Approval	Chief Operating Officer 20 May 2021
Endorsement	Pro Vice-Chancellor and President (Indonesia) 22 April 2021
Date effective	24 May 2021
Review date	24 May 2024
Version	1.0
Content enquiries	dataprotectionofficer@monash.edu