PRIVACY PROCEDURE

PURPOSE

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 graduates; and
- ensure the ongoing effective operation of the University.

This procedure outlines how the University ('us', 'our' or 'we') handles personal, sensitive and health information to comply with applicable privacy legislation. It also directs employees on the responsible collection and handling of personal information. The procedure supports the principle of responsible and transparent handling of personal information.

SCOPE

This procedure applies to:

- all personal, sensitive or health information regardless of how it is collected or stored;
- the management of all personal, sensitive and health information held by an Australian campus of the University and the University controlled entities in Australia; and
- all university students and employees including adjunct and honorary appointments are bound by this procedure, herein collectively referred to as 'you' for the purpose of this procedure.

This procedure does not apply to:

- personal information or data which is legitimately in the public domain;
- personal information an individual has made public;
- information that relates to corporate, government or business entities; or
- external websites that are linked to the Monash University website.

Employees and students studying at Monash University Malaysia should refer to local policies in relation to confidentiality or privacy.

Where this procedure is adopted by Monash College, it should be read in reference to Monash College.

PROCEDURE STATEMENT

1. Underlying principles

1.1 In the handling of personal information we will:

- collect only the information necessary to fulfil the functions and activities of the University;
- take reasonable steps to inform you of the purpose of collection and the use and disclosure of the personal information, through the use of privacy collection statements;
- use and disclose the personal information for the primary purpose, a reasonably expected related secondary purpose, as authorised by law or with your consent;
- take reasonable steps to ensure the personal information we hold is accurate, complete and up to date; and
- designate a University Privacy Officer responsible for overseeing the administration of our privacy compliance matters.

2. Collection of personal information – including sensitive or health information

2.1 We may collect personal, sensitive or health information from prospective and current students, employees and other individuals who interact with us. Only information that is necessary to fulfil the functions and activities of the University will be collected. Such collection will be by lawful and fair means and will not be unreasonably intrusive.

2.2 Sensitive and health information will only be collected if it is directly related to the primary purpose for which the information will be collected or as required by law or with your specific and informed consent.

2.3 The type of personal information collected will be determined by the nature of the interaction and contact with us. To provide more detailed information relating to the handling of personal information, we have adopted a number of central privacy collection statements based on the type of interaction.

2.4 We have adopted a number of central privacy collection statements. When collecting information a link to the appropriate specific privacy collection statement must be included.

2.5 Where practicable, we will collect personal information directly from you. In some cases we may collect information from a third party, such as Victorian Tertiary Admissions Centre (VTAC), another educational institution, an employment agency, a former employer, a contractor or a government authority such as Victoria Police.

2.6 Where personal information is provided to us by a person other than you, we will:

- de-identify or destroy the information if it is not to be retained; or
- if the information is to remain identified and be retained, provide the person to whom the information relates a copy of the relevant privacy collection statement explaining the purposes of collection, where such a statement has not already been provided.

3. Automatically collected information

3.1 Personal information may be automatically collected when you visit University campus or premises or use our websites, mobile applications, Wi-Fi and other online services. The types of information collected 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 information 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.

4. Use and disclosure of personal information

4.1 Information 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 and security of our premises generally and for the security of University students, employees and visitors;
- the provision of emergency or safety messages;
- in the course of addressing enquiries and requests; and
- for a secondary purpose or where permitted by the law.

4.2 More detailed information is outlined in the applicable privacy collection statement which are provided at the time personal information is collected or as soon as practicable thereafter.

4.3 In addition, personal information (including sensitive and/or health information) may be used or disclosed if 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 Your information may be disclosed to law enforcement and government bodies, insurers, University employees and contractors, third parties who provide services to the University or as required by law.

4.5 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 information.

4.6 If the proposed purpose for use or disclosure is not covered by the existing privacy collection statement please contact the University Privacy Officer for advice prior to the use or disclosure occurring.

5. Security and quality of personal information

5.1 We take reasonable steps to ensure that personal, sensitive and health information we collect, maintain, use or disclose is:

- accurate, complete and up to date;
- protected from misuse, loss, unauthorised access, modification or disclosure; and
- securely destroyed or permanently de-identified when no longer required in accordance with the Record Keeping 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 information 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 A login name and password are required to visit secure areas. You should ensure that your password is kept securely.

5.5 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 information as provided for by the privacy principles.

6. Access and correction of personal information

6.1 If you are a student or an employee, you should ensure your personal information is accurate, complete and up to date, through online systems such as the Web Enrolment System (WES) or Employee Self Service (ESS). If you are unable to access these systems, you should refer to Monash Connect (students) or Monash HR (employees) to update relevant personal information.

6.2 If you are a student who requires access to your information, including access to your student file, you should refer to the Privacy of Student Records policy and procedure. If you wish to access other personal documents not available under this policy, you must lodge a request in accordance with the Freedom of Information procedure.

6.3 If you are an employee seeking access to your personnel file, you may lodge a request in writing to the Chief Human Resources Officer, Monash HR. If you wish to access other personal documents not held on your personnel file, you must lodge a request in accordance with the Freedom of Information procedure.

6.4 Members of the public and former employees and former students should refer to the Freedom of Information Policy for access procedures.

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 information and will be handled accordingly.

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 personal information outside Victoria or (for controlled entities) outside Australia

9.1 Personal information may be transferred interstate or overseas 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 information collected and held by us may be transferred outside of Victoria (but within Australia) or outside Australia.

9.3 Where we transfer personal information outside Victoria, we take 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 information; or
- determining if the recipient is subject to legal or binding scheme that provides protection which is substantially similar to the applicable information privacy or health privacy principles; or
- contractual arrangements requiring the recipients of the information to handle information in accordance with the information privacy and health privacy principles; or
- seeking the consent of the individual prior to transferring the information; or
- as is otherwise permitted by law.

10. Responsibility for privacy compliance

10.1 Privacy compliance is the responsibility of all employees, students and other authorised users who handle personal or health information.

10.2 Employees must not knowingly direct another employee or student to handle (including disclosing) information in a manner which will breach privacy obligations.

11. Opting out of receiving material produced by the University

11.1 If you are an employee or student and you do not wish to receive communications from us, you can opt out by utilising the unsubscribe options on the specific publication.

11.2 Alternatively, a written request can be forwarded to the University's Privacy Officer at privacyofficer@monash.edu detailing the communications you no longer wish to receive.

11.3 Some University communications are not optional and must continue to enable the University to operate effectively.

12. Privacy Impact Assessments

12.1 A Privacy Impact Assessment (PIA) should 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 collection, use, disclosure or storage of personal or health information. A PIA is undertaken:

- to ensure legal obligations are met to protect the privacy of any personal and health information we collect, use, disclose, and store;
- to support good governance and informed decision making in the handling of personal and health information;
- to ensure appropriate risk mitigation considerations to the University, community and individuals in the handling of personal and health information 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.

12.2 Further information relating to PIAs is available here.

13. Privacy Complaints

13.1 If you are an employee or a student and are concerned your personal information has not been handled in accordance with this procedure, you should contact the Privacy Coordinator within the faculty/division who will seek to resolve the matter. A list of Privacy Coordinators is available here.

13.2 The Privacy Coordinator will then advise you what action, if any, we will take to resolve your concerns.

13.3 If you are not satisfied with the response of the Privacy Co-ordinator, you may lodge a written complaint to the University's Privacy Officer. Such complaint should include contact details, an outline of the issues relating to the alleged inappropriate handling of personal information and the remedy sought.

13.4 Members of the public may lodge a written complaint direct to the University Privacy Officer using the form available here.

13.5 Where necessary, the Privacy Officer will investigate the complaint and provide a response in writing to the complainant.

13.6 Written correspondence may be forwarded to the Privacy Officer at:

Privacy Officer, Monash HR
Monash University
211 Wellington Rd
Clayton Vic 3800
Email: privacyofficer@monash.edu

14. Privacy Incidents and reporting privacy incidents

14.1 Where employees, students or a member of the public is informed of, or becomes aware of a privacy incident, the incident should be reported directly to the University's Privacy Officer by email at privacyofficer@monash.edu for advice, assessment and possible investigation and response. For further advice regarding reporting of a privacy incident refer to or contact the Privacy Officer.

14.2 Where appropriate, the Privacy Officer will investigate the privacy incident, and provide a report on the outcome of the investigation and the actions recommended to address the incident to the Chief Operating Officer or nominee.

14.3 A privacy incident means a suspected or potential breach of the information Privacy Principles or Health Privacy Principles, including:

- the use or disclosure of personal or health information for a purpose that is not authorised by the individual or by law; or
- the loss, misuse, unauthorised access, modification or disclosure of personal or health information.

15. Breach of procedure

15.1 If a student or employee or other person breaches this procedure, depending on the circumstances it may be regarded as misconduct or unsatisfactory performance. In such cases, it may result in action being taken in accordance with the provisions set out in the applicable student conduct rules, Monash University Enterprise Agreement or contract terms.

15.2 We treat any breach of our policies or procedures seriously. We encourage reporting of concerns about non-compliance and manage compliance in accordance with the applicable Enterprise Agreement or contract terms.

16. Responsibilities

Employees

16.1 All University employees including adjunct and honorary appointees of the University are responsible for being aware of and complying with this procedure. Whilst there are some differences between the state and federal privacy legislation, employees of Monash controlled entities should also be aware of and comply with this procedure.

Students

16.2 Students are responsible for being aware of and complying with this procedure and keeping their details updated.

Faculty and divisions

16.3 Faculties and Divisions are responsible for:

- appointing a privacy coordinator for the faculty/division; and
- informing the University Privacy Officer of changes to privacy appointments.

Privacy Coordinators

16.4 Privacy Coordinators are responsible for:

- assisting employees, students and others with general queries regarding privacy;
- escalating queries and privacy complaints to the Privacy Officer where appropriate; and
- informing the University Privacy Officer immediately of privacy incidents.

University Privacy Officer

16.5 The University Privacy Officer is responsible for:

- providing expert assistance with interpretation and compliance regarding Privacy Laws and this procedure;
- managing privacy related queries, incidents and complaints;
- providing guidance to Privacy Coordinators on escalated privacy queries;
- as the delegate of the Chief Operating Officer, investigating privacy incidents and written complaints and reporting on the outcome of such investigations;
- developing and publishing supporting documents which assist employees in the application of this procedure; and
- coordinating privacy related training and education for University employees.

17. Further information and assistance

17.1 Employees, students or members of the public requiring assistance with the interpretation of the procedure should contact:

- The relevant Privacy Coordinator; or
- The University Privacy Officer on ext. 29589 or by email privacyofficer@monash.edu;
- The Office of the General Counsel on ext. 55126

DEFINITIONS

Health Information	Refer to Privacy Key Definitions
Personal Information	Refer to Privacy Key Definitions
Privacy Collection Statement	Statements used by the University to inform an individual of: • the purpose of collection of personal information, • the use and disclosure of the personal information, • their right to access their personal information, • how to contact the University, • whether the information is to be transferred outside of Victoria or Australia; and • the main consequences for the individual if the information is not provided.
Privacy Impact Statement	A privacy impact assessment is an assessment of any actual or potential impacts that an activity or project or system may have on the handling pf personal or health information.
Privacy Incident	A breach or potential breach of the Information Privacy Principles (IPPs) or Health Privacy Principles (HPPs), including, without limitation: • the use or disclosure of Personal Information or Health Information for a purpose that is not authorised by the individual or by law; or • the loss, unauthorised access or modification of Personal Information or Health Information.
Privacy Officer	The Chief Operating Officer who oversees privacy compliance by Monash University and delegates responsibility for the day to day administration of the privacy compliance arrangements to the University Privacy Officer for Victorian campuses, including to investigate and report findings in relation to privacy incidents, complaints and other privacy related matters. The Privacy Officer, in conjunction with the Office of the General Counsel will be responsible for updating this procedure and other supporting documents in accordance with changes in privacy legislation.
Sensitive Information	Refer to Privacy Key Definitions
Unique Identifier	Refer to Privacy Key Definitions

ADMINISTRATION

Parent policy	Integrity and respect
Supporting policies	• Electronic Information Security • Employment conditions • Equal opportunity • Ethics Statement • Leave and wellbeing • Pay, benefits and entitlements • Privacy of Student Records • Probation, performance and promotion • Recruitment and appointment
Supporting procedures	
Supporting documents	• Authorisation for Information Disclosure • Monash University Enterprise Agreement (Academic and Professional Staff) 2014 • Privacy at Monash • Privacy Guidelines and Monash University Privacy Collection Statements
Legislation mandating compliance	• Privacy and Data Protection Act 2014 (Vic) contains 10 Information Privacy Principles (IPP) which outline how personal information should be handled • Health Records Act 2001 (Vic) contains 11 Health Privacy Principles (HPP) which outline how health information should be handled • Freedom of Information Act 1982 (Vic) • Privacy Act 2000 (Cth) applicable to Monash University Controlled Entities (e.g. Monash College)
Responsibility for implementation	
Approval body	Chief Human Resources Officer
Procedure owner	Director, Workplace Relations
Date effective	20 March 2018
Review date	3 years from effective date
Category	Human Resources
Version number	5
Content enquiries	ask.monash or phone Monash HR on (03) 990 20400