Privacy Policy and Statement for MIT Students

1. Purpose of this document

This document describes the policy of Melbourne Institute of Technology Pty Ltd ("MIT") on how MIT collects, uses, discloses and otherwise handles "personal information", "health information" and "sensitive information" (collectively "information") about students, prospective students and former students ("you"). It also details how you may access personal information held by MIT about you and how you can lodge a complaint if you believe the privacy of your personal information has been breached.

2. Definition

Personal information is information or an opinion (including information or an opinion forming part of a database) about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in material form or not.

Sensitive information includes information or an opinion about an individual's racial or ethnic origin, or criminal record, that is also personal information; and, health information about an individual.

Health information includes information or an opinion about the health, including an illness, disability or injury (at any time) of an individual that is also personal information. We ask for information about the status of your health in accordance with the Health Privacy Principles and in consideration of your wellbeing whilst studying at MIT.

3. Australian Privacy Principles

MIT is bound by the Australian Privacy Principles (APPs) in Schedule 1 of the Privacy Act 1988 (Cth) (see http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/).The APPs provide standards, rights and obligations in respect of how personal information is handled from collection, to use, disclosure, storage and access. We are also bound by the requirements of the Health Privacy Principles under the Health Records Act 2001 (Vic) and Health Records and Information Privacy Act 2002 (NSW)

4. Collection of information

4.1. What kind of information does MIT collect and why?

MIT collects personal information for the primary purpose of providing its higher education services and for purposes related to the primary purpose to you. This includes:

- providing and administering approved courses, including admission, enrolment, teaching, assessment and payments;
- student services, including welfare programs and counselling services;

- student relations, including alumni;
- conducting surveys;
- compliance with reporting requirements and administration of government programs such as the Higher Education Loan Program;
- compliance with reporting requirements and administration of applicable laws and regulations of international students including under the Education Services for Overseas Students Act 2000, Migration Act 1958 and the Migration Regulations 1994.
- internal planning; and
- marketing the services of MIT and the promotion of MIT.

The personal information typically includes (but is not limited to): your name, age, gender, place of birth, nationality, contact details in Australia and other prescribed details; information about your course, financial arrangements and payments in relation to the course, health insurance, English language proficiency, passport, student visa, breach or suspected breach of visa conditions and academic progress and performance, and, information that MIT is obliged by law to collect or report.

If you do not provide the information as and when requested this may affect your enrolment at MIT.

4.2. How MIT collects information

MIT collects information by lawful and fair means, which are not unreasonably intrusive. MIT collects information that is reasonably necessary to perform its functions and activities or to comply with the law.

MIT generally collects information about you directly from you (eg. forms filled out by you, both paper and on-line or from meetings and interviews with you). MIT maintains records on each student which may include data on attendance, reports, marks and grades. There may also be times when MIT is provided with your personal information from a third party, such as through our partner institutions and from education agents who provide services to us. MIT will take reasonable steps to let you know, generally, what personal information it holds. MIT will seek your consent before collecting sensitive information unless collection is otherwise authorized or required by law.

4.3. Use and disclosure of information

MIT will only use or disclose personal information for the primary purpose for which it was collected, for any related secondary purpose that you would reasonably expect, or with your consent, or as permitted or required by law or as authorised by the APPs. MIT may use or disclose personal information (other than sensitive information) for the

purpose of MIT direct marketing, but must only do so in accordance with the APPs. MIT will only disclose health information in accordance with the Health Privacy Principles.

The following are examples where MIT discloses personal information for legitimate purposes:

- acquiring products and services which you authorize us to purchase for you, such as overseas student health care;
- offering and providing student support services (such as welfare related services, emergency and health services and complaints and appeals processes);
- publishing examination and assessment results;
- releasing academic details to another tertiary institution or tertiary admission centre if you apply for a transfer to another higher education institution;
- protecting you or someone else from a serious and imminent threat to life or health;
- disclosure that is reasonably necessary for the enforcement of the criminal law;
- in the event of an emergency, requiring disclosure to police, hospital or medical personnel.

MIT may disclose personal information to third parties for the purposes set out in this Privacy Policy, such as to a provider with whom we provide (or intend to provide or have provided) a course to you; an education agent; a person or body who sponsors you (if any); or any person entitled to the information or to any person to who you have authorised disclosure of your personal information.

MIT may also disclose personal information to third party service providers that MIT have retained to perform services on our behalf. When we do this, MIT will only provide them with such information as required to perform those services.

MIT may also use and disclose information where required or authorized by law (meaning any Commonwealth, State or Territory law or the common law) or in accordance with the APPs. For example, MIT may be required to disclose personal information about you to the Australian government and designated authorities (such as the Tuition Protection Service Director) if: you become an accepted student; you do not begin a course when expected; you withdraw from the course (before or after the agreed starting day); your studies are terminated before the completion of your course; you breach a prescribed condition of your student visa; or the identity or duration of your course changes.

4.4. Disclosure to overseas recipients

MIT may disclose your personal information to your nominated overseas education agent. These overseas recipients may be located in various countries. MIT shall comply with the APP's in respect of any disclosure of personal information to overseas recipients.

5. Protection of information

MIT holds personal information which may be stored in electronic and/or hardcopy form. MIT takes reasonable precautions to ensure that information is stored securely, is accurate and protected from misuse, loss, unauthorized access, modification or disclosure. MIT staff are bound by confidentiality on the use of personal information and are required to respect the privacy of individuals and MIT has in place ways to protect personal information including controlling access to MIT premises, security access to MIT's computer networks and other security technology. MIT may hold information about you while you are a student, and before and after you are a student. Where information is no longer needed and no longer required to be retained under legislation, MIT either destroys records containing personal information by reasonably secure means or de-identifies the personal information.

6. Data quality

MIT takes reasonable steps to confirm the accuracy of information it holds about you. From time to time, MIT asks for updated information including that required by legislation. MIT is not obliged to update information it holds about you after you have ceased your studies.

7. Access to information

You may request access to information that MIT holds about you by lodging a written request with MIT. The request must be made by you personally or by another person that you have authorised to make the request on your behalf. MIT may permit either inspection, note taking, copying or provide a print out of information, as it considers appropriate. Any request for access to personal information will be dealt within a reasonable period after the request is made and MIT may charge a fee for the cost of accessing and supplying the requested information. In limited circumstances MIT may refuse you access (see MIT's Terms and Conditions of Enrolment, Fee Payment and Refund Policy and as permitted under the APPs). In those cases, you will be notified of the reason MIT is refusing access.

8. Health Information

In handling your health information, MIT is bound by the Health Privacy Principles (HPPs) as set out in Health Records Act 2001 (Victoria) and Health Records and Information Privacy Act 2002 (NSW). MIT's approach to handling health information is detailed in the Health Privacy Principles Guidelines, annexed to this policy.

9. Queries or concerns and contacting us

Questions or concerns about the privacy of information we hold about you, and requests for access to and correction of personal information, and if you wish to make a complaint about a possible breach of privacy, may be directed to:

Melbourne Institute of Technology
288 La Trobe Street
Melbourne, Victoria 3000
E: privacy@mit.edu.au.
Tel: 03 8600 6700
Fax: 03 9010 0999
Complaints may also be directed to the Office of the Australian Information Commissioner (http://www.oaic.gov.au) if you think that MIT has interfered with your privacy.

Annexure: Health Privacy Principles Guidelines

1. Purpose

The purpose of this Guideline is to commit the Institute to the handling of health information in accordance with the Health Privacy Principles applicable under the Health Records Act 2001 (Victoria) and Health Records and Information Privacy Act 2002 (NSW).

2. Scope

The Guideline applies to all Institute students, including prospective and past students, and staff. Staff includes contractors and sessional staff, Executive Directors, external Board and Committee members, and visitors to the Institute.

3. Definitions

Term	Definition
health information	means personal information that is information or an opinion about: the physical or mental health or a disability (at any time) of an individual; or an individual's express wishes about the future provision of health services to him or her, or a health service provided or to be provided to an individual; or other personal information collected to provide, or in providing a health service, or other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or other personal information that is genetic information about an individual arising from a health service provided to the individual that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual, or healthcare identifiers, but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the

	purposes of this Act generally or for the purposes of specified provisions of the relevant Act (Health Records Act 2001 (Victoria) and Health Records and Information Privacy Act 2002 (NSW).
HPP	means Health Privacy Principles made under the Health Records Act 2001 (Victoria) and Health Records and Information Privacy Act 2002 (NSW), as applicable.
Privacy Officer	means the person designated the responsibilities associated with that of a Privacy Officer within the Institute.
Schedule	means the Schedules annexed to this Guideline, being: Schedule 1: HPP (Victoria); and Schedule 2: HPP (NSW).

4. Guideline Statement

In handling any health information, the Institute ("MIT") is bound by the Health Privacy Principles as set out in the Health Records Act 2001 (Victoria) and the Health Records and Information Privacy Act 2002 (NSW). This legislation created privacy rights that enables an individual to exercise greater control over how an organisation collects, uses and discloses health information that relates to them personally.

The Institute collects and uses information on health of staff and students in accordance with the HPPs. The HPPs set out requirements and obligations in handling health information, including the collection, use and disclosure, retention and security of health information, and an individual's right to access and make corrections to their health information.

The Institute is authorised to use certain health information in accordance with the principles contained in the following Health Privacy Principles:

Schedule 1: HPP (Victoria);

Schedule 2: HPP (NSW).

5. Responsibilities

5.1. The Institute-

The Institute will respond promptly to all queries or concerns relating to an Institute student or staff member's health information, together with requests for access to and correction of health information, or complaints.

On receipt of a request by a staff member or student the Institute must take reasonable steps:

- to let the individual know whether the Institute holds health information relating to the individual; and the steps that he or she should take if they wish to obtain access to the information; and
- if the Institute holds health information relating to the individual, to let the individual know in general terms the nature of the information; the purposes for which the information is used; and how the Institute collects, holds, uses and discloses the information.

5.2. Staff and Students

Institute staff and students may request access to their health information held by the Institute by lodging a written request, as detailed below. The request must either be made personally or by another person that the staff member or student has authorised to make the request on his or her behalf. The Institute may permit either inspection, note taking, copying or provide a print out of the health information, as it considers appropriate. Any request for access will be dealt with in a reasonable period after the request is made and the Institute may charge a fee for the cost of accessing and supplying the requested information. In limited circumstances, the Institute may refuse access. In those cases, the Institute will notify the applicant of the reason that is relying on to refuse access.

All correspondence should be directed to:

Melbourne Institute of Technology
288 La Trobe Street
Melbourne, Victoria 3000
E: privacy@mit.edu.au
Tel: 03 8600 6700
Fax: 03 9010 0999

Further complaints may also be directed to:

Victoria – Health Care Commissioner https://hcc.vic.gov.au/

NSW – Information Privacy Commissioner www.ipc.nsw.gov.au

5.3. Privacy Officer

The Privacy Officer is responsible for responding to requests for access to health information and for requests for correction, where found necessary. All requests will be

responded to within 20 days of receipt of the request and sufficient identification of the applicant.

6. Implementation and communication

This procedure will be implemented and communicated through the Institute via:

- Announcement on the Institute's webpage;
- Internal circulation to staff;
- Staff professional development;
- Student orientation programs;
- Student handbook.

Supporting documents and References

Government legislation:

Health Records Act 2001 (Victoria)

Health Records and Information Privacy Act 2002 (NSW).

Other;

MIT Privacy Policy and Statement

Schedule 1: Health Privacy Principles (Victoria)
HPP1 Collection - MIT must only collect health information if it is necessary for its functions and activities. Information is necessary only if there is a legitimate justification for its collection and at least one of the following applies: • the individual has consented, preferably in writing. • the collection is permitted by law. • the information is necessary to provide a health service to the individual and the individual is incapable of giving consent, and it is not reasonably practicable to obtain the consent of an authorised representative, or the individual does not have such an authorised representative. • The collection is for a secondary purpose directly related to the primary purpose and the individual would reasonably expect MIT to collect the information for the secondary purpose.

- MIT has reason to suspect that unlawful activity has been, or is being engaged in, and collects the information as a necessary part of its investigation of the matter or in reporting its concerns to the relevant persons or authorities.
- The information is collected about a deceased or missing person or a person involved in an accident who is unable to consent, and the health information is collected for the purposes of identifying the individual and contacting family members, unless this is against expressed wishes of the individual before they died, went missing or became incapable of providing consent.
- The collection is necessary for research in the public interest.
- MIT believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety and welfare or a serious threat to public health, public safety or public welfare.
- The collection is by or on behalf of a law enforcement agency and MIT reasonably believes that the collection is necessary for the law enforcement function.
- The collection is necessary for the establishment, exercise or defence of a legal or equitable claim

In addition MIT must only collect (including from a third party) health information by lawful and fair means and at or before the time of collection MIT must take reasonable steps to inform individuals of:

- the identity of MIT and how to contact it;
- the fact that he or she is able to gain access to the information;
- the purposes for which the information is collected;
- to whom, or the types of organisations to whom, MIT discloses information of this kind;
- any law that requires the particular information to be collected; and
- the main consequences (if any) for the individual if all or part of the information is not provided.

HPP2 Use and Disclosure - MIT may use or disclose health information collected at HPP1 for the primary purpose for which it was collected or a directly related purpose the individual would reasonably expect.

Health information can also be used or disclosed for a secondary purpose if:

- the individual has consented to the use or disclosure. Written consent is preferable.

- the use or disclosure is required or authorised by or under law. e.g. reporting communicable diseases.
- The use or disclosure by a health service provider is necessary to provide a health service and the individual is incapable of giving consent due to age, disability, mental disorder, etc. and there is no authorised representative available to provide consent.
- The use or disclosure is necessary for research in the public interest.
- MIT believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety and welfare or a serious threat to public health, public safety or public welfare
- MIT has reason to suspect that unlawful activity has been or is being engaged in and uses or discloses the health information to investigate the matter or to report concerns to relevant persons or authorities.
- A law enforcement agency has requested health information and authorisation has been obtained from the MIT Privacy Officer.

HPP3 Data Quality - MIT must take reasonable steps to make sure that health information it collects, uses or discloses is accurate, complete and up to date and relevant to its functions or activities.

HPP4 Data Security and Data Retention – MIT must take reasonable steps to protect the health information from misuse, loss, unauthorised access, modification or disclosure. Staff should ensure health information is not left lying around, that offices are locked, health information is stored in locked filing cabinets and passwords on computers are changed regularly.

Health information which is no longer needed should be de-identified. Deletion of health information is only permitted if:

- the deletion is permitted by law;
- if the health information was collected while the individual was a child, after the child reaches 25 years; or
- in any other case, more than 7 years after the last occasion on which the health service was provided.

If MIT deletes health information it must make a written note, which details the name of the individual, the period it related to and the date it was deleted.

HPP5 Openness – MIT must set out in a document clearly expressed policies on its management of health information. MIT must make the document available to anyone

who asks for it. The MIT Privacy Policy and Statement together with this Guideline have been developed as required by this HPP. On request by an individual, MIT must take reasonable steps to let that individual know generally what health information is held, for what purposes, and how it collects, holds, uses and discloses that information.
HPP6 Access and Correction - Individuals have the right to seek access to their personal information and make corrections. MIT will, on request, provide students and staff with access to information it holds about them and allow them to make corrections, unless an exemption applies at law. A valid explanation for refusal of access should be provided in writing. Exceptions include: where access would pose a serious threat to the life or health of any person, or would have an unreasonable impact on the privacy of other individuals.
HPP7 Identifiers – Unique identifiers (e.g. staff or student ID numbers) must only be assigned if it is necessary to allow MIT to carry out any of its functions efficiently.
HPP8 Anonymity - Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into a transaction with MIT.
HPP9 Transborder Data Flows – MIT may transfer health information about an individual to someone who is outside Victoria only if the organisation believes that the recipient of the information is subject to a law, binding scheme or contract, which effectively upholds principles for fair handling of information that are substantially similar to the HPP; or the individual concerned consents to the transfer; or the transfer is necessary for conclusion or performance of a contract in the interest of the individual between MIT and the third party. Transfers to NSW comply with Transborder Data Flow principles.
HPP10 Transfer or closure of the Practice of a Health Service Provider. Not applicable to MIT.
HPP11 Making Information available to another Health Service Provider. Not applicable to MIT.

Schedule 2: Health Privacy Principles (NSW)
HPP1 Purposes of collection of health information - Information must be collected by lawful means and for a lawful purpose directly related to a function or activity of the organisation and necessary for that purpose.

HPP2 Information must be relevant, not excessive, accurate (and up to date and complete) and not intrusive. The collection should not unreasonably intrude into an individuals personal affairs.
HPP3 Collection to be from individual concerned - MIT must only collect information directly from the individual, unless impracticable to do so. For example if a person lacks capacity.
HPP4 Individual to be made aware of certain matters – At or before the time when the health information is collected, or as soon as practicable after collection, MIT must take reasonable steps to ensure that the individual is aware of the following: • the identity of MIT and how to make contact; • the fact that he or she is able to gain access to the information; • the purposes for which the information is collected; • to whom, or the types of organisations to whom, MIT usually discloses information of this kind; • any law that requires the particular information to be collected; and • the main consequences (if any) for the individual if all or part of the information is not provided. MIT will make individuals aware by providing or publishing a collection notice, where appropriate.
HPP5 Retention and Security – Information is to be kept for no longer than is necessary and must be disposed of securely. MIT must take all steps to prevent loss, unauthorised access, use, modification or disclosure and all other misuse. MIT should have appropriate access restrictions in place: • Access to information is restricted according to level of responsibility within MIT; • Computer passwords are regularly changed; • Entry to buildings where important information is stored is by card access; • Sensitive information is securely stored and locked; • Offices unattended are locked; • Health information is stored away and not left exposed; and • Staff are aware of their privacy obligations.

HPP6 Information about health information held by organisations – MIT must provide enough detail about what health information it is storing, the main purposes for which it is used and the person's entitlement to request access to the information.
HPP7 Access – MIT must allow an individual to access his or her health information without excessive delay or expense. MIT may require that an application is in writing, and the application states the information being sought. An individual should direct an application to **admin@mit.edu.au**
HPP8 Amendment of health information – MIT must allow an individual to correct or amend information (including deletions) where necessary on request.
HPP9 Accuracy – MIT must not use information without taking such steps, as are reasonable in the circumstances, to ensure that the information is relevant, accurate, up to date, complete and not misleading.
HPP10 Limits on use of health information – Generally, MIT can only use an individual's health information for the purpose for which it was collected. The purpose for which the information was collected should have been communicated to the individual at the time when his or her information was collected, or as soon as practicable thereafter, in accordance with HPP 3. MIT may use the health information for other purposes where the individual: • consents to that use; or • where it is for a purpose directly related to the purpose for which it was collected and the individual would expect the organisation to use the information for that secondary purpose; or • where it is reasonably believed by the organisation to be necessary to prevent or lessen a serious and imminent threat to the life, health or safety of an individual, or serious threat to public health or safety.
HPP11 Limits on disclosure of health information – In the absence of consent from an individual, MIT may only disclose his or her health information to third parties where: • the disclosure is directly related to the purpose for which the information was collected and the individual would reasonably expect that MIT would disclose that information for that purpose; or • where MIT reasonably believes that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life, health or safety of you or another person or to lessen or prevent a serious threat to public health or public safety. MIT will only disclose an individual's health information to others when the circumstances are serious and impending, such as in a life threatening situation in which the individual is

involved, where the individual could be seriously injured or others might be injured as a result of the individual's actions. Some likely parties to whom an individual's information might be disclosed include the ambulance services or the police.
HPP12 Identifiers – unique identifiers (e.g. staff or student ID numbers) must only be assigned if it is necessary for MIT to carry out any of its functions efficiently.
HPP13 Anonymity - Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with or receiving health information from MIT.
HPP14 Transborder Data Flows – MIT may transfer health information about an individual to someone who is outside New South Wales or to a Commonwealth agency, only if MIT believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of information; or the individual concerned consents to the transfer.
HPP15 Linkage of health records - MIT must not link health information about an individual with health records of another, unless the individual has expressly consented to the disclosure.
MIT is not required to comply with HPPs 4,5,6,7,8,10,11 or 15 where it is lawfully authorised or required not to comply or where non compliance is permitted under law.