Privacy Policy

Section 1 - Purpose

(1) The purpose of this policy is to:

a. Define Melbourne Polytechnic's (MP) obligations for handling, personal sensitive information together referred as Personally Identifiable Information (PII) and/or health information referred as Protected Health Information (PHI) of former, current and prospective employees, students, visitors and all individuals with whom it has business dealings;
b. Outline MP employees' obligations and encourage all employees to take a proactive approach to privacy; and
c. Detail MP's obligations for investigating and responding to individuals' complaints related to privacy incidents/breaches.

Section 2 - Scope

(2) This policy applies to the collection, use, disclosure, storage and disposal of all PII & PHI that MP holds regarding MP's former, current and prospective employees, students, officers including board members and external committee members, contractors, volunteers, visitors, all individuals with whom it has business dealings; and persons who visit MP's website or social media accounts (who may be referred to throughout this policy as "you" or "your"). This policy also refers to procedures addressing unauthorised access, modification or loss of PII & PHI.

Section 3 - Policy

Policy Statement

(3) MP is committed to the responsible management of all the PII & PHI it holds. This commitment arises not only from the obligation for MP to comply with its legal and regulatory requirements but also in recognition of MP respect for the privacy rights of the members of its community.

(4) In undertaking its core functions of teaching and research, and in conducting the activities which support these functions, MP will balance the public interest in the free flow of information with the protection of the PII & PHI that MP collects.

Policy Principles

(5) MP recognises that privacy governance plays a critical role in:

a. Identifying and protecting PII & PHI held by MP;
b. Supporting and promoting accountability and transparency;
c. Supporting information confidentiality, integrity and availability;
d. Promoting efficient work practices; and
e. Supporting best business practices that align with MP's strategic direction and Victorian privacy compliance

obligations.

Policy Topics

Privacy Standards

(6) This policy will be guided by the following standards:

a. Proactive privacy – MP is proactive in its approach to privacy protection by anticipating and preventing invasive events before they occur;
b. Privacy by design – MP embeds privacy considerations into the design and architecture of information technology systems and business processes;
c. MP collects, uses, discloses and manages all PII & PHI as MP records in accordance with the relevant legislation (see Appendix A – Relevant Legislations).

Collection

(7) MP collects, manages and shares your information as required to undertake its operational functions and related activities. More information on the areas/functions in which your PII & PHI may be collected (see Appendix B).

(8) MP is only permitted to collect your PII & PHI in a transparent, lawful, fair manner that is not unreasonably intrusive.

(9) MP collects your personal and health information:

a. Where necessary and relevant to MP's functions and activities; or
b. Where required by law; or
c. Where you or your authorised representative have consented.

(10) MP is only permitted to collect your sensitive information where you or your authorised representative have provided consent, or where the collection:

a. Is required by law;
b. Is otherwise authorised under the Privacy and Data Protection Act 2014 (Vic) or the Health Records Act 2001 (Vic).

(11) When collecting PII & PHI directly from an individual, whether by verbal, written or electronic means, MP will take all reasonable steps to ensure that the individual providing such information is made aware of how their information will be used and with whom it might be shared or communicated in an appropriate collection statement or consent notice when applicable.

(12) In relation to the handling of your PII & PHI by MP, further information is available in Current & Prospective Employees Personal Information Collected (see Appendix C) and the Student Privacy Statement.

(13) The Senior FOI and Privacy Adviser will develop and maintain a series of collection statements to inform individuals of the ways in which MP uses and discloses, and may reasonably anticipate MP to use or disclose, their PII & PHI.

(14) MP will take all reasonable steps to not collect PII & PHI from individuals, if it is reasonable and practicable to transact with them without collecting this type of information.

Use and disclosure

(15) In the course of its activities, MP will take all reasonable steps to only use PII & PHI collected for:

a. The primary purpose of collection; or
b. A related secondary use reasonably anticipated by the individual; or
c. Where an individual has consented; or
d. Where authorised by law.

(16) MP's employees and associates are only permitted to access relevant PII & PHI to the extent necessary to perform their job.

(17) MP will not share your PII & PHI with other third parties without your prior consent unless this is required by law or with governmental or educational agencies where release of that information is relevant to the proper work of the particular organisation. Authorised disclosures of relevant parts of your personal information with your consent will be made to organisations nominated by you for an identified purpose such as for the deposit of your salary.

Data security and disposal

(18) MP takes all reasonable steps to:

a. Protect information it holds from misuse, loss and unauthorised access, modification and disclosure, including through software safeguards and controls, restricted access and assignment of roles and responsibilities;
b. Ensure all information is destroyed or permanently de-identified when it is no longer needed by MP in compliance with the Public Records Act 1973 (Vic), MP Records Management Policy and all relative legislations.

(19) MP takes all reasonable steps to ensure its contracted service providers comply with all privacy laws that apply to MP.

Anonymity

(20) Where practicable and lawful, you may interact with MP anonymously (and you can use a pseudonym as long as you tell MP that it is a pseudonym). However, this will limit MP's ability to assist you or provide services to you.

a. For example, if you choose to:
    i. Make a complaint anonymously, MP will be unable to contact you, seek further information, or let you know the outcome of any complaint process if the complaint is investigated in compliance with the Student Complaints and Appeals Policy or Fraud and Corruption Prevention Policy; or
    ii. Make course enquiries anonymously, MP will be unable to facilitate your enrolment in a course or provide related services.

Accuracy

(21) Generally, MP relies on you to provide accurate information and to notify MP if you believe that information is inaccurate, incomplete or outdated. MP will take reasonable steps to remedy this after being notified.

Access and correction

(22) An individual has the right to request that MP provides them with access to, or an opportunity to correct their PII & PHI held by MP, by contacting the relevant department or person listed in the Access & Correction Request table.

TO ACCESS OR CORRECT INFORMATION	CONTACT DETAILS
If you have queries, questions complaints or others and you are: a. Domestic Students: enrolment or contact details b. International onshore students: enrolment or contact details c. Current students: • Counselling • Disability support • Gym membership • Recreational activities including Student Life at MP (SLAM), sport and excursions d. Prospective or former students: contact details	Student Hub Complete the online request form at https://melbournepolytechnic.secure.force.com/ComplaintsProStudentEnquiry and attach evidence as required
Current students: • Attendance • Special consideration • Training and assessment	Your Teachers, Program Leads, or Academic Managers Your teacher will provide contact details on request
Library access and borrowing	Manager Library and Learning Skills Post: Locked Bag 5, Preston VIC 3072 Email: library@melbournepolytechnic.edu.au
Prospective, current or previous employees	Executive Director, People, Culture and Corporate Services Post: Locked Bag 5, Preston VIC 3072 Email: info@melbournepolytechnic.edu.au

(23) MP may refuse access where required or authorised by law. In some cases, MP may advise you to make a request in accordance with the Freedom of Information Act 1982 (Vic) (such as where your request involves information regarding third parties). See MP's factsheet regarding freedom of information, available on our corporate website.

(24) To protect your privacy and the privacy of others, MP requires appropriate evidence of your identity and/or proof of accurate and current delegation before it can consider a request for access or correction.

Data Subject Rights of European Economic Area/United Kingdom Residents

(25) In addition to the rights of access and correction above and subject to any conditions and exemptions in the GDPR, MP will respect the rights of residents of the European Economic Area and the United Kingdom to:

a. Object to processing of their PII & PHI;
b. Request suspension of processing of their PII & PHI;
c. Transfer their PII & PHI held in electronic form to them or a third party in a structured, commonly-used, machine-readable form; or
d. Withdraw their consent to processing where MP's right to process is based only on their consent.

Transfer of PII outside Victoria or Australia

(26) Your information may be transferred outside Victoria or outside Australia where:

a. You or your authorised representative have consented;
b. It is necessary to perform services for you;
c. MP has taken reasonable steps to ensure the information will be handled consistently with Victoria's privacy laws; or
d. Where required or permitted by law.

(27) Consent may be implied in certain circumstances, such as where you are studying or working outside of Australia.

Digital Content and Third-Party Platforms

(28) MP shares information and engages with you and the community by:

a. Operating the website domains www.melbournepolytechnic.edu.au and www.melbourneamep.com.au
b. using a variety of social media applications such as Twitter; Instagram; Facebook; YouTube; and MP Thrive app
c. making online academic support services available to officers, employees, contractors, contracted service providers and students, including Studiosity, Moodle and Zoom.

(29) Please refer to the Melbourne Polytechnic Privacy Statement on MP's websites for further details about how your information is handled.

(30) Regarding applications and services owned by third parties that have their own privacy practices and procedures which are different to MP's, MP will take all reasonable steps to ensure the security of your PII & PHI in compliance with Privacy Laws.

Blended Learning and Teaching (Videoconferencing)

(31) MP remains aware that a blended learning and teaching experience must still recognise the need for privacy for both MP's employees, associates and students, and complies with all regulatory obligations as set out in the present Privacy Policy.

(32) Further information on privacy requirements and Blended Leaning is available in the Zoom Recording Privacy Notice.

Privacy Impact Assessment

(33) MP undertakes Privacy Impact Assessment as part of a proactive risk management strategy, to assist employees in identifying information management and security risks, and in identifying and evaluating solutions to mitigate those risks in compliance with the Privacy Impact Assessment Procedure.

(34) Risks identified in PIAs will be entered into Protecht by the Senior FOI and Privacy Adviser to ensure appropriate management of those risks.

Procurement & Contracts

(35) All contracts entered into by MP:

a. Must follow an approved procurement process including internal review/consultation of the contract by the Information Management and Security team to ensure third-party vendors' privacy and security compliance with all Victorian privacy laws including but not limited to the Privacy and Data Protection Act 2014 (Vic);

b. Must include provisions related to appropriate safeguards for protection of Personal and Health Information. Advice from the Senior FOI and Privacy Adviser must be sought where PII & PHI is to be transferred outside of Australia.
c. Must follow the Privacy Impact Assessment Procedure.

Breaches

(36) Breaches of policy compliance may result in disciplinary action being taken against the offender respectively in accordance with the Employment Policy, the Personal Information Management Procedure, the Code of Conduct Policy, the Acceptable Usage (Students) Policy, the Information Technology Resources (All Users) Policy, Information Security Awareness Policy and all related policies and procedures of MP and all related policies and procedures of MP.

(37) Substantiated Breaches will be reported to the Risk and Compliance Department and entered into Protecht by the Incident Manager.

Complaints

(38) An individual has the right to complain to the Senior FOI and Privacy Adviser via email privacy@melbournepolytechnic.edu.au about the unauthorised use, access, disclosure, modification or loss of their PII & PHI by MP, whether deliberate or inadvertent. A complaint will be managed in accordance with the provisions of the Privacy Breach Management Guideline.

(39) An individual who believes that MP has engaged in an act constituting an interference with their privacy may make a privacy complaint to MP in accordance with subclauses a-d.

(40) Complaints should be made within six (6) months of the time the complainant first became aware of the alleged breach;

(41) Where the complainant is a currently-enrolled student or recent graduate (12months) of MP, any complaint will be dealt with under the Student Complaints and Appeals Policy;

(42) Where the complainant is an employee of MP, any complaint will be dealt with under the Employee Grievances Policy;

(43) Where the complainant is neither a currently-enrolled student, a recent graduate (12 months) nor a current employee, complaints must be forwarded in writing to the Senior FOI and Privacy Adviser via email privacy@melbournepolytechnic.edu.au. The Senior FOI and Privacy Adviser will be responsible for:

a. Appointing an appropriate person to undertake an investigation of the complaint and to provide recommendations for an appropriate response to the appointed Investigator;
b. Determining the actions MP will take;
c. Providing a written response in respect of the outcome to the complainant, and
d. Advising relevant MP personnel of actions required to remedy the interference with the complainant's privacy (if any).

(44) MP will make every effort to provide a result of its review to the complainant within 60 days of receiving a detailed and complete complaint. If you are not satisfied with MP’s response to your 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.

Section 4 - Responsibility and Accountability

(45) All MP employees, and associates of MP will be responsible for performing the duties of their employment, appointment or engagement by MP, in accordance with the following principles:

a. Respect the privacy of personal and health information that they collect, use or disclose;
b. Comply with the requirements of all applicable personal data protection laws, this policy, and its related procedures and guidelines including the Personal Information Management procedure.
c. Take all reasonable steps to keep the information secure including adopt a respectable behaviour that wouldn't impinge the security and safety of MP's network nor the privacy of other students or employees while:
    i. Being on MP premises;
    ii. Accessing MP network including all Digital Learning and Teaching environments supported by MP for education purposes such as Moodle, and Zoom;
    iii. Using MP's devices, especially by complying with the requirements of all applicable personal data protection laws, the Student Code of Conduct Guidelines
    iv. Complying with the Information Technology Resources (All Users) Policy, this policy, the Acceptable Usage (Students) Policy and its related procedures.
d. Report any suspected privacy or data breach to the Information Management and Security Team in compliance with the Privacy Breach Management Guideline.

(46) All MP employees and associates will be responsible to:

a. undertake and complete the induction privacy training, the annual privacy training modules and periodical refreshers from the beginning of their employment to the release of their duties, ensuring MP meets its privacy requirements and obligations;
b. meet screening checks including national police clearance, background (employment history) and misconduct checks commensurate with their roles and responsibilities and/or access to PII & PHI at the beginning of employment / engagement which must be renewed on a periodical manner in compliance with the Screening Policy.

(47) The Senior FOI and Privacy Adviser will be responsible for:

a. Controlling and maintaining the Privacy Policy;
b. Administering this policy, including conducting Privacy Impact Assessments (PIAs), monitoring compliance, informing training and assisting employees on privacy issues, responding to requests concerning the access to any PII & PHI or privacy complaints and investigating potential privacy breaches;
c. Being the contact point for the purposes of the GDPR.

Section 5 - Supporting Documents and Templates

(48) Related MP policies and procedures:

a. Acceptable Usage (Students) Policy
b. Authentication Policy
c. Employment Policy
d. Employee Grievances Policy
e. Information Asset Policy

f. Information Security Awareness Policy
g. Information Security Classification Policy
h. Information Technology Resources (All Users) Policy
i. Personal Information Management Procedure
j. Privacy Breach Management Guideline
k. Privacy Impact Assessment Procedure
l. Records Management Policy
m. Records Management Procedure
n. Social Media Policy
o. Screening Policy
p. Student Code of Conduct Guidelines
q. Student Discipline Policy
r. Student Privacy Statement
s. Working with Children and Police Check Policy

(49) Related Legislation and Regulation:

a. Accident Compensation Act 1985 (Vic)
b. Audit Act 1994 (Vic)
c. Charter of Human Rights and Responsibilities Act 2006 (Vic)
d. Child Wellbeing and Safety Act 2005 (Vic)
a. Crimes Act 1958 (Vic)
a. Disability Act 2006 (Vic)
b. Do Not Call Register Act 2006 (Cth)
c. Education and Training Reform Act 2006 (Vic)
d. Education Services for Overseas Students Act 2000 (Cth)
e. Equal Opportunity Act 2010 (Vic)
f. Fair Work Act 2009 (Cth)
g. Financial Management Act 1994 (Vic)
h. Freedom of Information Act 1982 (Vic)
i. Health Records Act 2001 (Vic)
j. Higher Education Support Act 2003 (Cth)
k. Income Tax Assessment Act 1997 (Cth)
l. Independent Contractors Act 2006 (Cth)
m. Long Service Leave Act 2018 (Vic)
n. National Vocational Education and Training Regulator Act 2011 (Cth)
o. Occupation Health and Safety Act 2004 (Vic)
p. Ombudsman Act 1973 (Vic)
q. Privacy Act 1988 (Cth)
r. Privacy and Data Protection Act 2014 (Vic)
s. Public Administration Act 2004 (Vic)
t. Public Records Act 1973 (Vic)
u. Racial and Religious Tolerance Act 2001 (Vic)
v. Spam Act 2003 (Cth)
w. Student Identifiers Act 2014 (Cth)

x. Superannuation Guarantee (Administration) Act 1992 (Cth)
y. Superannuation Industry (Supervision) Act 1993 (Cth)
z. Tertiary Education Quality and Standards Agency Act 2011 (Cth)
aa. VET Student Loans Act 2016 (Cth)
ab. Victorian Data Sharing Act 2017 (Vic)
ac. Workers Compensation Act 1958 (Vic)
ad. Working with Children Act 2005 (Vic)
ae. Workplace Injury Rehabilitation and Compensation Act 2013 (Vic)

(50) Templates

a. Collection Notice Template
b. Privacy Impact Threshold Assessment Template
c. Privacy Impact Assessment Template (Full Report)

Section 6 - Definitions

(51) For the purpose of this policy the following definitions apply:

a. Blended Learning and Teaching: means that students will be connected to learning and assessment through a combination of in-person and technologically enabled experiences.
b. Confidential Information: all data, in its original and duplicate form, for which there is either a legal, ethical, or contractual requirement to restrict access. Confidential information must be restricted to those with a legitimate business need for access. For example: financial information, system access passwords, building plans, tenders and contracts, information about a third party with whom Melbourne Polytechnic has a commercial relationship, etc.
c. Data & Privacy Breach: Unauthorised access, misuse, disclosure or loss of any Confidential Information, Personal Information or Sensitive Information held by Melbourne Polytechnic. Data Breach refers to any type of information whereas privacy breach relates to any PII & PHI.
d. Digital Learning and Teaching environment: means an education environment in which digital technologies are electronic tools, systems, devices and resources that are integrated into a learning and teaching environment that is collaborative; enables learning that is inclusive; in the best interests of the students and, creates opportunities for all learners using different delivery modes. It is a learning experience that requires a combination of technology, digital delivery of content, and teachers and students working in a collaborative approach to gaining knowledge and skills. Common examples include Moodle and Zoom sessions.
e. Employees: refers to all former, current and prospective employees, officers, agents, contractors and subcontractors of MP.
f. Health Information: means information or an opinion about
    i. your physical, mental or psychological health;
    ii. any disability you may have; or any health service provided or
    iii. proposed to be provided to you.
g. Notifiable Data Breach scheme (NDB): means eligible data breaches that fall under the Commonwealth mandatory reporting scheme. As a Tax File Number Recipient, this applies to MP in relation to any unauthorised access to, or unauthorised disclosure of, tax file number data.
h. Protected Health information (PHI): Protected health information (PHI), also referred to as personal health information, is a subset of personally identifiable information that specifically refers to the demographic information, medical histories, test and laboratory results, mental health conditions, insurance information and

other data that a healthcare professional collects to identify an individual and determine appropriate care.

i. Personally Identifiable Information (PII): collectively or individually refers to Personal Information, Sensitive Information, Health information, and identifiers.

j. Personal Information: refers to information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable. Common examples are an individual's name; age; date of birth; contact details; address, bank account details, medical records, image (as recorded in video footage or a photograph).

k. Privacy Impact Assessment: means a risk analysis tool to identify and mitigate privacy and data protection risks, and to identify and evaluate privacy solutions.

l. Sensitive Information: refers to information or an opinion about your race; ethnicity; political opinions; trade union memberships; religion; sexual preferences; or criminal record.

Status and Details

Status	Historic
Effective Date	31st August 2023
Review Date	31st August 2026
Approval Authority	Chief Executive
Approval Date	4th May 2023
Expiry Date	12th December 2023
Policy Owner	Daryl Sadgrove Executive Director Strategy Performance and Growth
Policy Implementation Officer	David Glimsholt Director, Information Management and Security
Author	David Glimsholt Head Information Management and Security
Enquiries Contact	David Glimsholt Director, Information Management and Security