

Acceptable Usage (Students) Policy

Section 1 - Purpose

(1) This Policy sets out the requirements and expectations of students when using Melbourne Polytechnic (MP) Information Communication Technology (ICT) resources including networks.

Section 2 - Scope

(2) This Policy applies to all enrolled students of MP, regardless of their location or mode of study (on or off campus and within or outside Australia).

Section 3 - Policy

Policy Statement

(3) MP is committed to providing access to Information and Communications Technology (ICT) resources to support its community core functions of teaching, learning and research while ensuring the use of MP ICT resources is legal, ethical and consistent with the aims, values and objectives of MP and its responsibilities to staff, students and other ICT users.

Policy Principles

(4) This Policy will be guided by the following principles:

- a. MP provides access to ICT resources to support the academic and educational pursuits of enrolled students.
- b. Students are encouraged to use these ICT resources to broaden their understanding and application of contemporary technologies, to enhance their studies and to assist them to engage positively and actively with communities and individuals primarily, but not exclusively, for purposes linked to their study.
- c. Access to MP's ICT resources is a privilege. Students must use these resources responsibly and in compliance with all applicable laws, ethical standards, and the behavioural expectations outlined in the MP [Student Discipline Policy](#).
- d. Students must use MP ICT resources in accordance with their appropriate authorised purposes. Unauthorised software must not be installed on the computers.

(5) This Policy clearly defines the activities that are strictly prohibited when using ICT resources at MP; including engagement in activities that harass, threaten, or intimidate others, including cyberbullying, and any action that violates MP's academic integrity policies. Such activities can result in harm to individuals, damage to the MP's reputation, and the creation of a hostile academic environment.

(6) Furthermore, any activities that interfere with the normal operation of ICT resources, such as intentionally overloading the network with non-academic activities, are prohibited. This ensures that the ICT resources remain available for academic pursuits, and there is no disruption of the academic process. Students are also prohibited from attempting to gain unauthorised access to ICT resources. Such activities can compromise the integrity of MP's ICT

resources and threaten the privacy and security of the academic community.

(7) Lastly, the policy prohibits accessing, distributing, or receiving material that is illegal, inappropriate, or offensive. Such materials can create an unwelcoming environment for the academic community and may expose the institution to legal and reputational risks.

(8) By using ICT resources at the institution, students acknowledge that they have read and agree to comply with this policy. This Policy will be updated regularly, and students will be notified of any changes.

Policy Topics

Email Acceptable Use

(9) All students are provided with an MP email address (studentid_no@student.mp.edu.au), which will only be available while students are enrolled at MP. Students and parents/guardians of students under the age of 18 should be aware that the MP provided email address will be the primary mode of communication between MP and individual students. Students must check their student email account regularly as a condition of their enrolment. They can choose to forward their email account to a personal email address.

(10) MP supplied email addresses should only be used for purposes related to individual student's study and not be used to register for any personal services, or with inappropriate or suspicious web sites or mailing lists, as this can often contribute to the receiving of SPAM emails.

(11) Students should be vigilant with the content of their MP mailbox and prevent sending personal and private information on their MP account.

(12) ICT Resources must not be used to offend another person based on their race, gender, or any other attribute prescribed under anti-discrimination legislation.

(13) When communicating via email or messaging services, students must not send messages that a reasonable person would consider rude, antagonistic, bullying, threatening, offensive or humiliating.

(14) Messages that do not meet professional standards may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures, including:

- a. [Student Complaints and Appeals Policy](#)
- b. [Student Equal Opportunity, Discrimination and Harassment Policy](#)

Acceptable Use - Safety & Security

(15) The use of ICT resources is controlled with an account linked to a "user id", assigned access rights and protected by a personal password. Passwords must remain confidential. Students will be held responsible for any unauthorised use of their accounts. To help keep your access secure:

- a. Create a unique password for your MP mailbox that is different from passwords used for other accounts you hold;
- b. Keep your passwords confidential (i.e. do not share them with other students or third parties);
- c. Adhere to MP mandated minimum password length and complexity rules and optional multifactor authentication (MFA), which is recommended for all students;
- d. Log out of the network whenever not in use or leaving your workstation. Do not leave your laptop unattended for even a short period of time while being logged on MP's network;
- e. Ensure that only fully licensed and approved software are installed on MP computers, and report any suspect software to your lecturer/teacher or any employees;

- f. Do not modify any spam and filtering settings that have been applied to MP's computers and ensure any personal devices you connect to MP's networks have up to date protection software (such as antivirus);
- g. Provide a valid proof of identification (i.e. student card, driving license, or passport) when using computing facilities, requesting access to services or upon request of by an MP employees (i.e staff members).

ICT Resource Acceptable Use

(16) Students are authorised to use MP's ICT resources primarily for activities related to their academic pursuits at MP. Examples of authorised uses include, but are not limited to:

- a. Accessing course materials
- b. Conducting research
- c. Communicating with staff and other students
- d. Completing assignments and assessments
- e. Participating in online learning environments
- f. Participating in online discussions

(17) Each student must respect the right of others to work and/or study in an environment which is free from harassment and intimidation when using MP's ICT resources.

(18) Personal use of MP's ICT resources for services such as email or web access is permitted where this is kept to a minimum and will not cause disruptions to other services or users.

(19) Students should only access information and systems for which they are authorised and must not bypass any protective controls or attempt to access, use or disclose information that is noticeably addressed to MP employees or other students.

(20) Students should be aware that transferring excessively large files can have an adverse effect on network resources and negatively affect classroom delivery. This practice is strongly discouraged.

Online Privacy Acceptable Use

(21) When using ICT resources, students must always act in a safe, responsible and ethical manner by:

- a. Respecting others and communicating with them in a supportive manner; never writing or participating in online bullying (for example, forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviours);
- b. Protecting your privacy; not giving out personal details, including your full name, telephone number, address, passwords or images;
- c. Protecting the privacy of others; never posting or forwarding their personal details or images without consent;
- d. Talking to a teacher/lecturer when feeling uncomfortable or unsafe online, or when witnessing others participating in unsafe, inappropriate or hurtful online behaviours;
- e. Investigating the terms and conditions of use for any digital or online tools (e.g. age restrictions, consent requirements); and
- f. Seeking further explanation from your teacher/lecturer or Student Services when clarification is needed.

Unacceptable Use of ICT Resources

(22) In alignment with Melbourne Polytechnic's policies (including the social media policy), the following uses of IT resources are strictly prohibited:

- a. Any activity that violates local, state, or federal laws or regulations, including but not limited to:
 - i. Using MP ICT infrastructure to access, use, copy or transmit copyright material, confidential or sensitive information or personal information related to other individuals (students/teachers, etc) without the explicit consent of the information owner;
 - ii. Forging MP documents or documents submitted to MP;
- b. Any activity that violates MP's academic integrity policies, including but not limited to:
 - i. Plagiarism, cheating in exams, and falsifying academic records, among others;
 - ii. Falsely claiming or using an identity, qualification, prior learning or experience;
- c. Any activity that is intended to harass, threaten, defame or intimidate others, including but not limited to:
 - i. Using MP's ICT resources to threaten, harass, defame or offend others, or to discriminate against others
 - ii. Using MP's ICT resources in a vilifying, sexist, racist, abusive, annoying, insulting, threatening, obscene or any other offensive manner;
- d. Any activity that interferes with the normal operation of ICT resources, including but not limited to:
 - i. Introducing malicious computer code (e.g., viruses, worms, Trojan horses, ransomware, etc.) designed to self-replicate, damage or otherwise hinder the performance of any ICT Resource;
 - ii. Effecting security breaches or disruptions of network communication;
 - iii. Circumventing user authentication or security of any host, network or account;
 - iv. Using network penetration, hacking tools or any software that could compromise the security and privacy of the network or its users;
- e. Any activity that is intended to gain unauthorised access to ICT resources, including but not limited to:
 - i. Accessing data, systems or accounts for any purpose unrelated to legitimate educational, administrative, or approved institutional activities.
- f. Any activity that is intended to damage, modify, or destroy ICT resources, including but not limited to:
 - i. Tampering or moving ICT resources without prior express authorisation;
 - ii. Attempting to interfere or alter system configurations or corrupt, damage or destroy data and other physical or digital assets;
 - iii. Misusing ICT resources; care must be always exercised when using ICT resources, students will be held responsible for the cost of repair if damage is caused through misuse or negligence;
- g. Any activity that is intended to distribute, receive, or access material that is illegal, inappropriate, or offensive, including but not limited to:
 - i. Attempting to transfer, store or print files, material or messages that violate anti-discrimination legislation, copyright law or MP policies and procedures;
 - ii. Downloading, displaying or transferring offensive material, including material that is sexist, sexually explicit, pornographic or racist using MP's ICT resources;
- h. Inciting another person to commit any of the above.

Exceptions to Prohibited Activities

(23) The following activities are strictly prohibited, except under the following conditions: they are part of a course curriculum; are performed in segregated controlled classroom environment; are performed under the supervision of a qualified teacher; and have obtained written authorisation by Director, ICT Services (CIO) and Director, Information Management and Security (IM&S):

- a. Conduct port scanning or security scanning
- b. Executing any form of network monitoring which will intercept data
- c. Introduce or execute any network penetration, hacking tools or any software that can find and exploit

weaknesses in computer systems, web applications, servers and networks.

Reporting Receipt of Offensive Material

(24) Students who receive unsolicited offensive material from an unknown external source or a known source within MP must report it immediately to the relevant Head of School or Program Manager who will determine if the Director, ICT Services (CIO) and/or Director of IM&S is/are to be advised.

(25) Students may also lodge a complaint to express dissatisfaction with the quality of an action taken or decision made by another MP student, employee, and or third party.

(26) Students must not print or forward offensive material.

Violation of the Policy

(27) Violations of this policy may result in disciplinary action in compliance with the [Student Discipline Policy](#), including but not limited to:

- a. Suspension or revocation of ICT resource access, including but not limited to: Prohibiting the student access to or use of MP premises, MP facilities and services or MP activities for up to two weeks;
- b. Confiscation of any evidence that may indicate a student has committed, is committing or intends to commit misconduct;
- c. Academic penalties, such as failing grades or academic suspension, including but not limited to:
 - i. Receiving a formal warning. A student can only receive two warnings for the same offense
 - ii. Signing an Acceptable Use Agreement;
 - iii. Completing an agreed course of corrective actions which can include counselling, or refraining from contact with specified persons;
 - iv. Suspension of the student for up to two weeks;
 - v. Prevention of the student from re-enrolling, receiving results, graduating or receiving an award.
- d. In addition to any disciplinary action by MP, a student's serious misconduct may lead to civil or criminal proceedings and penalties (when evidence of illegal conduct has occurred), which MP may report to relevant law enforcement bodies and for which the student will be held personally accountable.

(28) A student who fails to comply with a sanction under this Policy is guilty of serious or repetitive misconduct.

(29) Serious or repetitive misconduct may lead to disciplinary action, including the revocation of student account or suspension from MP in compliance with MP [Student Discipline Policy](#).

(30) A serious misconduct will result in automatic denial of access to one or all facilities and will be referred to the Course facilitator or Program Lead.

(31) In some exceptional circumstances (for example where access to objectionable material relates directly to a user's employment or study with MP), subject to the approval of and at the discretion of authorised persons, an exemption may be granted for activities that would otherwise breach these guidelines. Exemptions may be required to be approved in advance by the Head of Management Unit.

(32) When serious misconduct is suspected, MP reserves the right to audit and remove any illegal material from its computer resources at its discretion.

Access, monitoring, filtering and blocking

(33) MP does not generally monitor email, files, internet downloads or data stored on ICT Resources. However, the

Institute reserves the right to access and monitor ICT Resources and network traffic for security, compliance, and other purposes, including investigating suspected breaches of this policy or unlawful activities. Staff undertaking investigative procedures must adhere to MP's [Code of Conduct Policy](#). Such activities include, but are not limited to:

- a. Monitoring email, chat, and other communications
- b. Reviewing logs and usage reports
- c. Conducting audits and investigations
- d. Enforcing this Policy and other relevant policies

(34) Students must acknowledge that:

- a. The use of ICT systems and resources are premised on the condition that their use may be monitored;
- b. MP has the right to access, monitor, filter and block electronic communications created, sent or received by any user using the systems;
- c. Student access is provisioned when commencing at MP, and student access will be removed and/or restricted 6 months after graduation or withdrawal from a course.

Bring Your Own Device (BYOD)

(35) Students may use a personally owned device such as a laptop, tablet or smart phone to access MP Systems and Services.

(36) When using a personally owned device, students must ensure the security requirements and device specifications outlined in the MP [BYOD Standard \(Students\)](#) are followed.

ARTIFICIAL INTELLIGENCE (AI)

(37) MP supports the responsible, safe and ethical use of AI technologies by staff and students to enhance learning, productivity, and operational efficiency, in line with all applicable policies, privacy requirements, and legal obligations.

(38) All AI use must demonstrate responsible, ethical, and safe practices, ensuring outputs are accurate, ethical, and consistent with the MP's [Guiding Principles for Artificial Intelligence](#) summarised below:

- a. Professional responsibility- ensuring AI use is designed and implemented in accordance with professional understanding, capability and responsibility by staff and students.
- b. Fairness and inclusion – advocating for fair and inclusive use of AI, avoiding biases and discrimination in both access to AI and content produced from or by AI.
- c. Transparency and explainability – ensuring AI is utilised with transparency and explainability, aligning with values that emphasise integrity, honesty, and respect for human dignity. This includes AI use disclosure and understandable AI inputs and outputs.
- d. Privacy, safety and security – ensuring AI is used with appropriate consideration of the safety and wellbeing of staff and community in line with Australian federal and state law(s), MP policies and any other applicable standards, laws and regulations.
- e. Accountability – ensuring AI use upholds academic integrity, respects cultural and intellectual property, while maintaining human accountability for decisions and making sure outputs are justifiable and verifiable
- f. Human control and the promotion of human values – making sure AI use safeguards human control, upholds human dignity and values, supports education and professional growth, and enhances human thought and experience.

Full details are available on MP's Artificial Intelligence student portal: [AI for students](#)

(39) AI use must align with all relevant MP Policies, Procedures and Guidelines as well as applicable Victorian and

Australian laws and regulations, along with those of the user's applicable jurisdiction (e.g. offshore staff and students).

(40) MP has identified the following broad categories of AI Platforms available to students and staff:

- a. MP Approved AI Platforms:
 - i. These are AI platforms that have undergone formal assessment and are approved for use at MP. Examples include Microsoft Copilot.
 - ii. Approved AI platforms provide AI enabled capabilities while ensuring that sufficient controls over data access, handling, privacy protections, and regulatory compliance, are in place to manage associated risks.
 - iii. MP approved AI platforms should be used for learning and other academic activities, as these platforms have been assessed for safety and regulatory compliance.
- b. Public AI Platforms:
 - i. Public AI platforms refer to AI systems that are publicly accessible via the internet and have not been formally assessed or recommended for use at MP. Examples include online personally subscribed or free platforms not provided by MP.
 - ii. Where possible, MP approved platforms must be used ahead of public AI platforms.
- c. Banned AI Platforms:
 - i. These are public AI platforms assessed as High Risk by MP or other regulatory bodies and are prohibited for use on MP devices and networks. An example is Deepseek, for onshore students (based in Australia).
 - ii. Some AI platforms available in Australia may not be available internationally. Offshore students (i.e. studying from outside of Australia) may be permitted to use other platforms provided approval is sought prior to use.

(41) Approved AI Usage:

- a. Students may use AI tools to support their learning unless use of AI is explicitly restricted or prohibited by MP, such as in the assessment instructions, subject outline or lecturer/teacher instructions.
- b. Students must use MP-approved AI platforms, where possible. However, they may use public AI platforms tools for Low Risk activities providing they do not upload MP-associated data when doing so. MP associated data includes learning materials, assessment questions, rubrics, student information, emails, class discussion content, or other institutional materials.
- c. Where AI is used in a learning context, there should be appropriate staff oversight, especially in the case of students under 18 years of age.

Data Management and Handling When Using AI

(42) Students must not share sensitive information, such as Personally Identifiable Information (PII) and Personal Health Information (PHI) with the AI tools, to reduce risk of unintended disclosure.

(43) Students must respect all Intellectual Property (IP) rights. AI-generated materials must not infringe third-party copyright or breach MP's IP ownership and reuse requirements. MP provided learning materials should only be used with MP approved AI tools unless authorised to use public tools.

(44) Any suspected breach, AI misuse, or unauthorised data disclosure must be reported immediately via the [Student Portal](#) (lodge a ticket) or call 1300 635 276, and will be handled in line with MP's [Information Security Incident Response Policy](#), [Academic Integrity Policy](#) and [Procedure](#), and [Student Discipline Policy](#).

Accountability on AI Generated Materials

(45) Students remain fully responsible for the accuracy, appropriateness, and ethical integrity of all AI materials they produce, use or distribute.

(46) Students must understand AI's inherent limitations and uncertainties, and critically evaluate the credibility of AI generated content against trusted sources and evidence, addressing any errors, inconsistencies, or biases; before using, distributing, relying upon, or incorporating into learning activities, including assessment tasks.

Attribution and Disclosure of AI Use

(47) Students are required to always comply with the Institute's [Academic Integrity Policy](#) requirements, including in situations where AI use is permitted in assessments and other academic work.

(48) Where AI is used, students must acknowledge or cite AI use in accordance with assessment instructions and/or relevant citation requirements.

(49) Students must clearly attribute any AI-generated or AI-influenced content used in their work (e.g. in assessments), identifying the tool and nature of AI involvement where appropriate.

AI Training, Awareness and Support

(50) Students are expected to complete undertake any AI training provided or endorsed by the Institute as part of their studies.

(51) Students may seek guidance or support regarding the use of AI by consulting their educators, the Student Hub, or by lodging a support request ticket to Student Support (via [Student Portal](#) or call to 1300 635 276).

AI Legal and Regulatory Compliance

(52) All Students are required to uphold Australia's AI Ethics Principles in all cases where AI is used, including in learning, scholarly activity and assessment practices.

(53) Students are required to familiarise themselves with all applicable Australian laws, regulations, standards and guidance and ensure AI use align with these.

(54) Students must ensure the use of generative AI tools comply with any terms set out by the provider of the tool and this may include an age limit.

(55) For underage students (under 18), opt-in consent must be provided by their parents and carers before using AI tools that require personal information beyond provision of their Melbourne Polytechnic email address and creation of a password for registration.

Prohibited Uses of AI

(56) The following uses of AI are strictly prohibited:

- a. Any AI use that violates ethical boundaries, academic integrity, MP's [Student Code of Conduct Guidelines](#), or [MP privacy, data security, and copyright/IP policies](#).
- b. Sharing of Personally Identifiable Information, Protected Health Information or MP-owned materials and data, with AI tools.
- c. Generating content for exams or assessments where AI use is not permitted.
- d. Uploading media including depictions of other students, staff or parents (for example, photos, audio, video), or generate images or other media in the likeness of these people.

- e. Generate artefacts that mimic a cultural tradition in a way that is disrespectful or offensive (for example, images mimicking Koorie artwork).
- f. Creation or dissemination of:
 - i. deepfakes, deceptive manipulated media, or intentionally misleading content.
 - ii. content contrary to policies and procedures, bullying, harassment, discriminatory, misinformation illegal, offensive, inappropriate materials or interactions.
- g. Use of banned AI Platforms.
- h. Installing, executing, or use unauthorised AI agents or automation tools (including those deployed via scripts, package managers, containers, or user-profile directories) on MP devices or connecting such tools to MP systems or data without formal approval.

Section 4 - Responsibility and Accountability

(57) Students are responsible for:

- a. Ensuring that the use of MP ICT resources complies with MP's Policies and Procedures;
- b. Ensuring responses to email correspondence occur within a reasonable timeframe. This may include correspondence redirected to students' personal email addresses for ease of access;
- c. Seeking redress for any form of harassment or intimidation resulting from inappropriate use of MP's computer network by MP students or employees through the [Student Complaints and Appeals Policy](#).

(58) Information Management and Security (IM&S) Team and Digital and Technology Experience (DTE) are responsible for:

- a. Investigating breaches of proper use of MP systems and network;
- b. Investigating and mitigating all data breaches;
- c. Granting exemptions to this policy (Such as those specified in paragraph 22).

(59) All MP employees are responsible for reporting and assisting in the investigation and mitigation of suspected breaches.

Section 5 - Related Policies and/or Procedures

(60) [Academic Integrity Policy](#)

(61) [Academic Integrity Procedure](#)

(62) [Social Media Policy](#)

(63) [Student Code of Conduct Guidelines](#)

(64) [Student Complaints and Appeals Policy](#)

(65) [Student Discipline Policy](#)

(66) [Student Privacy Statement](#)

(67) [Video Conferencing Policy](#)

Section 6 - Definitions

(68) For the purpose of this Policy the following definitions apply:

- a. Artificial Intelligence (AI): refers to technologies, systems, or tools that perform tasks normally requiring human intelligence. These include generating content, making predictions, identifying patterns, performing language or image processing, or assisting with decision-making.
- b. AI Platform: any software, application, or online service that uses AI technologies to generate, analyse, or process data.
- c. Access Rights: Defines the level a user is provided around the read, modification, and execution of files on one or more systems.
- d. Complaint: an expression of dissatisfaction with the quality of an action taken, decision made, or service provided by MP, contractors or third-party providers, or a delay or failure in providing a service, taking an action, or making of a decision by MP, its contractors or a third-party provider.
- e. Corrective Action: Action taken to address an issue or resolve a complaint or appeal.
- f. ICT systems and Resources: MP's computer infrastructure. It includes all computers and computing devices (including both the wired and wireless local area networks) as well as any software services provided by MP for student use.
- g. Malicious Computer Code: harmful computer code or web script designed to cause damage, security breaches or other threats to application security.
- h. Misconduct: any behavior that goes against your code of conduct or other policies that dictate how students should behave. This might include unethical, unprofessional, or even criminal behavior.
- i. Multi Factor Authentication: an electronic authentication method in which a user is granted access to an application or system after successfully presenting two or more pieces of evidence to an authentication mechanism: something you know (Password / Passphrase), something you possess (token, mobile phone, etc.), or something you are (Biometrics).
- j. Password: A sequence of characters used for authentication.
- k. Penetration Testing Tools: Software and hardware-based tools that verify the extent to which a system, device or process resists active attempts to compromise its security.
- l. 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).
- m. Personally Identifiable Information (PII): collectively or individually refers to Personal Information, Sensitive Information, Health information, and identifiers.
- n. 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.
- o. Port Scanning: A method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.
- p. Security Breach: Any incident that results in unauthorized access to computer data, applications, networks or devices.
- q. Serious Complaint: Refers to a complaint which includes, but is not limited to allegations and/or incidents that:
 - i. require MP to take direct action (e.g. sexual harassment, threat of harm to self or others).
 - ii. are potential offences under law that could be proven (e.g. actual or alleged sexual, physical or other

assault); or

iii. may otherwise present a significant risk to MP, its students, staff and/or community.

- r. SPAM: Irrelevant or unsolicited messages sent over the internet, typically to many users, for the purposes of advertising, phishing, spreading malware, etc.
- s. Unauthorised Software: includes, but is not limited to; games, instant messaging and chat programs, file transfer and peer-to-peer file sharing programs.
- t. Users: Enrolled students of MP, and former students whose enrolment ended no more than 12 months before the date the incident occurred; and/or former students whose access hasn't been revoked.

Status and Details

Status	Current
Effective Date	6th August 2026
Review Date	31st July 2031
Approval Authority	Chief Executive
Approval Date	31st July 2026
Expiry Date	Not Applicable
Policy Owner	Joseph Santiago Executive Director Finance, Reporting, Assurance and Marketing
Policy Implementation Officer	David Glimsholt Director, Information Management and Security
Author	David Glimsholt Director, Information Management and Security
Enquiries Contact	David Glimsholt Director, Information Management and Security Information Management and Security