Acceptable Usage (Students) Policy

Section 1 - Purpose

(1) This policy sets out the requirements and expectations of students when using Melbourne Polytechnic (MP) Information Technology (IT) 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 provide access to 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 Information Communication Technology (ICT) systems and software resources to enrolled students to support the academic and educational pursuits of enrolled students.
b. Students are encouraged to use these IT 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. Students are advised that with the opportunity to use MP’s IT resources comes the responsibility to behave legally, ethically, morally and according to the standards of behaviour outlined in MP Student Discipline Policy.
d. Students must use MP computing and communications systems in accordance with their appropriate authorised purposes. Unauthorised software must not be installed on the computers.
e. This policy clearly defines the activities that are prohibited in the use of IT resources at MP. Such activities include engaging in any action that violates MP's academic integrity policies. Engaging in activities that harass, threaten, or intimidate others, including cyberbullying, is strictly prohibited. Such activities can result in harm to individuals, damage to the MP's reputation, and the creation of a hostile academic environment.
f. Furthermore, any activities that interfere with the normal operation of IT resources, such as intentionally overloading the network with non-academic activities, are prohibited. This ensures that the IT 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 IT resources. Such activities can compromise the integrity of MP's IT resources and threaten the privacy and security of the academic community.
g. 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.

h. By using IT resources at the institution, students acknowledge that they have read and agree to comply with this policy. This policy may be updated from time to time, and students will be notified of any changes.

Policy Topics

Email Acceptable Use

(5) 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 manually forward their email account to a personal email address. Please note the automatic forwarding of emails from your MP email address to a personal one will be disabled for security measures.

(6) MP supplied email addresses should only be used for purposes related to your own 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.

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

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

(9) 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.

(10) 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 Procedures
b. Student Equal Opportunity, Discrimination and Harassment Policy

Acceptable Use – Safety & Security

(11) The use of IT 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. MP enforces minimum password length and complexity rules and offers 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 on request of a employees.

IT Resource Acceptable Use

(12) Students are only authorised to use MP's IT resources 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
g. Each individual 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 IT resources.
h. Personal use of MP's IT 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.
i. 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.
j. 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

(13) When using digital technologies, students must act in a safe, responsible and ethical manner always 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 they feel 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 (g. age restrictions, consent requirements); and
f. Seeking further explanation from your teacher/lecturer or Student services when your understanding is unclear.

Unacceptable Use of IT Resources

(14) 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 IT 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 IT resources to threaten, harass, defame or offend others, or to discriminate against others
    ii. Using MP’s IT resources in a vilifying, sexist, racist, abusive, annoying, insulting, threatening, obscene or other offensive manner;

d. Any activity that interferes with the normal operation of IT 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 IT 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 IT resources, including but not limited to:
    i. Accessing data, a server or an account for any purpose other than for learning and studying purposes, even if you have authorised access.

f. Any activity that is intended to damage, modify, or destroy IT resources, including but not limited to:
    i. Tampering or moving IT assets 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 IT equipment; care must be always exercised when using IT equipment, 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 IT resources;

h. Inciting another person to commit any of the above.

Exceptions to Prohibited Activities

(15) 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 ICT and 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

(16) 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 of

ICT and/or Head of Information Management & Security is/are to be advised.

(17) 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.

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

Violation of the Policy

(19) 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 IT 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, student’s serious misconduct may lead to civil or criminal proceedings and penalties (when legal offense), which MP may report to relevant law enforcement bodies and for which the user will be held personally accountable.

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

(21) 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.

(22) 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.

(23) 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.

(24) When misconduct is suspected, MP reserves the right to audit and remove any illegal material from its computer resources without discretion.

Access, monitoring, filtering and blocking

(25) MP does not generally monitor email, files, internet downloads or data stored on IT Resources. However, the Institute reserves the right to access and monitor IT 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

(26) Students:

a. Use the systems on the understanding and condition that their use may be monitored;
b. Acknowledge and consent to MP's right to access, monitor, filter and block electronic communications created, sent or received by any user using the systems;
c. Acknowledge that 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.

Section 4 - Responsibility and Accountability

(27) Students are responsible for:

a. Ensuring that the use of MP resources and computer network complies with MP's Policies and Procedures;
b. Ensuring email correspondence is responded to within a reasonable timeframe. This may include correspondence redirected to student personal email address 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.

(28) Information Management and Security (IMS) and Information Communication Technology (ICT) Services are responsible:

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 14)

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

Section 5 - Supporting Documents and Templates

(30) Related MP policies and procedures:

a. Privacy Policy
b. Social Media Policy
c. Student Code of Conduct Guidelines
d. Student Complaints and Appeals Policy
e. Student Discipline Policy
f. Student Privacy Statement
g. Video Conferencing Policy.

Section 6 - Definitions

(31) For the purpose of this procedure the following definitions apply:

a. Access Rights: Defines the level a user is provided around the read, modification, and execution of files on one or more systems
b. 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.
c. Corrective Action: Action taken to address an issue or resolve a complaint or appeal.
d. IT 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.
e. Malicious Computer Code: harmful computer code or web script designed to cause damage, security breaches or other threats to application security.
f. 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.
g. 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).
h. Password: A sequence of characters used for authentication.
i. 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.
j. 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.
k. Security Breach: Any incident that results in unauthorized access to computer data, applications, networks or devices.
l. 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.
m. SPAM: Irrelevant or unsolicited messages sent over the internet, typically to many users, for the purposes of advertising, phishing, spreading malware, etc.
n. Unauthorised Software: includes, but is not limited to; games, instant messaging and chat programs, file transfer and peer-to-peer file sharing programs.
o. 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	10th May 2023
Review Date	4th May 2028
Approval Authority	Chief Executive
Approval Date	4th May 2023
Expiry Date	Not Applicable
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