Acceptable Usage (Staff) Policy

Section 1 - Purpose

(1) This Policy sets out the acceptable use of Melbourne Polytechnic (MP) Digital and Tech Experience (DTE) resources, including networks.

Section 2 - Scope

(2) This Policy applies to all users of MP DTE resources including Board and Committee members, employees, contractors, employees of any contractors, volunteers and guests (Users). This Policy excludes student users for which a separate Acceptable Usage (Students) Policy is available.

(3) This Policy applies to use of all MP DTE Resources, as defined below, located at campuses, office spaces, and in private homes or at any other location. It includes the following resources provided or funded by MP:

a. MP's communication networks.
b. Computer systems and software including PC's, tablets and servers.
c. Printers, copiers and multi-function devices (MFDs).
d. Cloud services.
e. Mobile phones and related mobile devices (g. smart phones, wireless data cards etc.)
f. Internet and social media.
g. Email, telephones and related communication services.

Section 3 - Policy

Policy Statement

(4) MP is committed to providing access to DTE resources to improve and enhance learning and teaching, and for the conduct of the business and functions of MP in a manner that is legal, ethical, and consistent with the aims, values and objectives of MP and its responsibilities to staff and other IT users.

(5) Users are expected to use and manage these resources in an appropriate manner and in accordance with this policy.

Policy Principles

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

a. MP provides access to DTE resources to all users to improve and enhance learning and teaching, and for conducting business and operational activities at MP.
b. Access to MP DTE resources is controlled using User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all their

actions on the institute's DTE resources.

c. All users must take responsibility for using DTE resources in an ethical, secure and legal manner having regard for MP objectives and the privacy, rights and sensitivities of other people.
d. All users must use MP DTE resources in accordance with their appropriate authorised purposes only.
e. This Policy clearly defines the activities that are prohibited in the use of DTE resources at MP. Such activities include:
    i. engaging in any action that violates MP's internal policies or any local, state, or federal laws or regulations that could result in harm to individuals, damage to the MP's reputation, and the creation of a hostile working environment.
    ii. engaging in any activities that interfere with the normal operation of DTE resources that could compromise the integrity of MP's DTE resources and threaten the privacy and security of the academic community.
    iii. accessing, distributing, or receiving material that is illegal, inappropriate, or offensive that can create an unwelcoming environment for the academic community and may expose the institution to legal and reputational risks.
f. By using MP DTE resources, users acknowledge that they have read and agree to comply with this policy. This Policy may be updated from time to time, and users will be notified of any changes.

Policy Topics

Business Use

(7) MP DTE resources are provided to users for business purposes. Other than limited personal use, MP DTE resources must be used for business purposes, or where authorised by MP management or required by law.

(8) Users are allowed reasonable access rights to electronic communications using MP DTE resources to facilitate communication between employees and their representatives, provided that the use is not unlawful, offensive, improper or resulting in the breach of any MP policies and procedures including MP's Code of Conduct Policy.

(9) Large data downloads or transmissions should be minimised to ensure the performance of MP DTE systems for other users is not adversely affected.

Personal Use

(10) MP DTE resources can be used for limited, incidental personal purposes as long as usage does not:

a. violate any MP policy or procedure,
b. negatively impact upon work performance,
c. interfere with business operations,
d. damage the reputation, image, or operations of the Institute, or
e. result in additional cost to the Institute.

(11) MP accepts no responsibility for personal usage that results in the:

a. loss or damage arising from personal use of DTE Resources, or
b. loss of data or interference with personal files arising from its efforts to maintain the DTE Resources.

Prohibited Conduct

(12) In alignment with MP's policies, the following uses of DTE resources is strictly prohibited:

a. Any activity that violates local, state, or federal laws or regulations, including but not limited to:
    i. accessing, using, copying or transmitting copyright material.
    ii. accessing, using, copying or transmitting confidential or sensitive information or personal information related to other individuals (Staff, students, teachers, etc) without the explicit consent of the information owner.
    iii. Forgery of MP documents or documents submitted to MP.
    iv. Using MP DTE resources for fraudulent activities.
b. Any activity that is intended to harass, threaten, defame or intimidate others, including but not limited to:
    i. Using MP's DTE resources to harass, defame, offend or discriminate against others.
    ii. Using MP's DTE resources in a vilifying, sexist, racist, abusive, annoying, insulting, threatening, obscene or other offensive manner.
c. 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.
d. Any activity that interferes with normal operation of DTE 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 DTE Resource.
    ii. Installing unapproved software programs on the MP computers that may impact integrity of MP systems and network.
    iii. Effecting security breaches or disruptions of network communication.
    iv. Circumventing user authentication or security of any host, network or account.
    v. Using unauthorised network penetration, hacking or scanning tools or any software that could compromise the security and privacy of the network or its users.
e. Any activity that is intended to or could result in gaining unauthorised access to DTE resources, including but not limited to:
    i. Accessing data, a server or an account for any purpose other than for than conducting MP business, even if you have authorised access.
    ii. Accessing data, a server, or a system to which the user is not authorised to.
    iii. Revealing or sharing your account password with others or allowing use of your account by others. This includes work colleagues, family, and other household members when work is being done from home.
f. Any activity that is intended to damage, modify, or destroy DTE equipment, including but not limited to:
    i. Tampering or moving DTE equipment 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 DTE 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. Inciting another person to commit any of the above.

Cloud Computing

(13) Cloud services are permitted to store, process or transmit MP data provided they are assessed to meet MP information security requirements and formally approved.

(14) It is the responsibility of the System Owner (requesting service), in consultation with the Information Owner, DTE

Services, General Counsel (Legal Counsel) and Information Management and Security (IM&S) to determine whether a particular cloud service and its provider (CSP) can suitably maintain the required level of security and regulatory compliance on an ongoing basis. Guidance should be sought from MP Third-Party Information Security Risk Procedure.

(15) The contractual agreement between MP and CSP must clearly specify contractual data protection terms that ensure that MP data is appropriately kept confidential, is not modified without prior consent from MP's representatives, and is available to the institute as needed.

Email and Internet Services

Internet/Web Usage

(16) Access to the Internet is provided to MP staff for conducting business activities and incidental personal use. Any access by staff that is inconsistent with business needs or could result in the misuse of resources is strictly prohibited. These activities may adversely affect productivity and may result in MP facing loss of reputation and possible legal action due to other types of misuse.

(17) MP filters and records any attempted access to Internet websites and protocols that are deemed inappropriate. The following list examples of categories of websites that may be blocked by MP:

a. Child Abuse.
b. Discrimination, Alternative Beliefs, and other Advocacy Organizations.
c. Alcohol and Drug Abuse.
d. Gambling, Sports Hunting and War Games.
e. Explicit Violence, Extremist Groups, Weapons (Sales).
f. Hacking, Proxy Avoidance, Phishing, Spam URLs.
g. Unethical Plagiarism.
h. Malicious Websites, Newly Observed Domain and Newly Registered Domain.
i. Adult/Mature Content, Nudity and Risqué, Pornography, Dating and Sex Education.

(18) If a website is mis-categorised, staff may request the site be removed from filtering by raising a ticket to the DTE Service Desk. Information Management and Security & DTE will review such requests in consultation with People and Culture, and Legal Services and permit access if the site is deemed mis-categorised and safe.

Email Usage

(19) All work email communications must be undertaken using MP email accounts(@melbournepolytechnic.edu.au). This includes communication with students who must be contacted via their official student email account(@student.mp.edu.au) and no other personal email address.

(20) Third-party email systems (such as Gmail, Hotmail, etc.) and storage servers (such as Dropbox, Google Drive) must not be used to conduct MP business including the storage of any MP related information. Additionally, Users are prohibited from automatically forwarding MP email to these third-party email providers. Any individual email messages that are forwarded by the individual to a third-party email provider must not contain MP confidential information.

(21) MP email may be used for limited personal communication; however, staff must understand that email communications and social media are not private and should not expect privacy undertaking these activities. Notwithstanding, all personal information shared or stored remain personal information and should be treated as such.

(22) When using MP email system, users must:

a. ensure emails containing MP's confidential or sensitive information are classified as "confidential", encrypted

during transmission, and digitally signed by the sender to ensure confidentiality and integrity.

b. not send messages that a reasonable person would consider rude, discriminatory, antagonistic, bullying, threatening, offensive or humiliating.
c. ensure professional standards are adhered to. Messages that do not meet professional standards may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures, including:
    i. Employee Grievances Policy
    ii. Equal Opportunity, Discrimination and Harassment Policy
    iii. Student Complaints and Appeals Procedure
    iv. Student Equal Opportunity, Discrimination and Harassment Policy

(23) All emails sent from MP staff accounts will automatically have a legal disclaimer attached to them. It should be noted that the disclaimer does not preclude MP or the sender of the email from being liable for its contents.

(24) Electronic communications including email and chat messages created on, sent or received using MP systems are the property of MP and may be accessed as part of an investigation. This includes investigations following a complaint or investigations into misconduct in compliance with MP's policies, including but not limited to, Student Complaints and Appeals Policy, Prevention of Workplace Bullying Policy, Fraud and Corruption Prevention Policy and Code of Conduct Policy.

(25) Staff should note that electronic communications of current and former staff may be subject to discovery in litigation and criminal investigations. All information produced on users' computers, including emails, may be accessible under the Freedom of Information Act 1982 (Vic) in compliance with MP's FOI Factsheet.

Fax Usage

(26) When sending faxes containing MP information from MP MFDs, the sender must ensure:

a. Arrangements are made for the receiver to collect the fax message as soon as possible after it is sent; and
b. The receiver must notify the sender if the fax message does not arrive in an agreed amount of time.

Social Media

(27) When using social media for private purposes (i.e. not via a MP branded account), Users must ensure:

a. any comments relating to MP activities must state they are not official, and that Users are providing a personal opinion ONLY,
b. any personal comments made do not compromise the capacity to perform their duties and
c. MP's trademarks, logos and any other intellectual property are not used.

(28) Comments posted on behalf of the Institute (i.e. via a MP branded account) must be compliant with all MP policies.

(29) MP's policies around confidential information apply to social media, as such, all users are prohibited from revealing any confidential or proprietary information, trade secrets, public sector information, or any other material covered by MP's Privacy Policy through any social media platform or public forums.

(30) Users should familiarise themselves with MP's Social Media Policy and ensure their activities online are in alignment with the policy.

Misrepresentation, impersonation and false labelling

(31) Staff must be aware that misrepresentation, impersonation and false labelling will lead to a breach of this policy

and MP's Privacy Policy, this includes altering communications to convey false messages, impersonate sender identities, or recipients, using false labelling or trademarks. In such cases, individuals might unknowingly engage with impostors, expose sensitive information or act on fraudulent information.

(32) If a user doubts the validity of a received message or the identity of the sender, they should take steps to verify the identity of the sender or validity of the message using alternative methods such as calling them. Users should notify their immediate manager or DTE or Information Management and Security (IM&S) if they suspect interception or modification of electronic messages.

(33) Users are responsible for all activities conducted on MP DTE resources or through their MP accounts. Users should therefore continuously monitor activities and the physical access to their DTE resources, including laptops, mobile phones, tablets, and notebook computers and report any suspected unauthorised activities or access.

(34) Users must ensure security controls to protect their ICT resources are followed consistently, including the following:

a. keeping their identification and passwords confidential,
b. terminating active sessions once they are no longer needed,
c. locking their computers and devices with passwords when not in use, and
d. keeping their computers and devices in a secure physical location when not in use.

Data and Information Storage

(35) Information and records storage practices must comply with MP's Records Management Policy and Records Management Procedure .

(36) All information or records created, received, or managed by users must be retained until the minimum retention timeframe has been met. This may involve:

a. Retaining records identified as Normal Administrative Practice (NAP) until reference ceases.
b. More information in how to identify a NAP record is available in Guideline – Records Destruction.
c. Retaining short- or long-term temporary records until minimum retention timeframes designated by the Public Record Office Victoria (PROV) have been met.
d. Retaining designated records permanently.

(37) Once information and records have met their minimum retention timeframe(s) and appropriate disposal approvals have been provided, they can be disposed of in accordance with MP's Records Management Policy and Procedure

(38) Any information or records created, received or managed by users relating to their work at MP must be saved in Institute approved storage locations (either on premise or in the cloud).

(39) In order to prevent risk of malware infections and loss of sensitive information, MP will not permit the use of removable media without the explicit permission of Information Management and Security. In the event that a removable media is required for performance of staff duties or when providing information required by state or federal authorities, DTE may provide the removable media to be used.

(40) Any sensitive information stored on removable media must be secured in accordance with the MP's Records Management Policy and Records Management Procedure.

Copyright Infringement

(41) Copyrighted material from third parties must not be used without the owner's prior written permission or

copyright licence when applicable (accessible on the owner's website copyright page). This may include software, database files, documentation, cartoons, articles, graphic files, music files, video files, books, text downloaded information and any copyrighted materials. MP staff must send all written permissions to the copyright@melbournepolytechnic.edu.au mailbox for record keeping before using the material.

(42) Forwarding, distributing, and sharing electronic messages, attachments and files greatly increases the risk of copyright infringement and users must assess the authenticity of the file ownership before distributing.

(43) Copying material to electronic storage, or printing, distributing, or sharing copyright material by electronic means may give rise to personal or MP liability, despite the belief that the use of such material was permitted.

Dealings in Copyright Protected Material for Teaching of Research

(44) All users of MP DTE resources (including those dealing with Copyrighted teaching and research materials) should be familiar with all relevant intellectual property and copyright guidelines provided by MP including the Copyright Requirements for the Development of Teaching Resources Policy and MP Intellectual Property Policy.

Confidentiality and Privacy

(45) The use, collection and disclosure of personal information when using DTE resources e.g. e-mail increases the risk of privacy and security breaches

(46) All MP users must handle personal information MP is the custodian, in compliance with the Privacy Policy and information handling procedures to ensure its appropriate protection. This includes and is not limited to the use, the disclosure and the restricted access to appropriate personnel of all personal information when using DTE resources.

(47) Only the minimum amount of personal information necessary to accomplish the purpose for which it is required should be transferred by e-mail.

(48) MP will not disclose the content of any internal electronic communications created, sent or received on MP DTE resources to third parties unless that disclosure complies with the Privacy and Data Protection Act 2014 (Vic) and is related to:

a. An MP investigation,
b. An investigation by law enforcement agencies,
c. For legal, audit or compliance reasons or
d. Or as required by law.

Access, monitoring, filtering and blocking

(49) MP does not generally monitor staff emails, files, internet downloads or data stored on DTE Resources. However, the Institute reserves the right to access and monitor DTE Resources and network traffic for operations, maintenance, security, compliance, auditing, legal, and other purposes, including investigating suspected breaches of this policy or unlawful activities.

(50) Access to the information gathered from the monitoring of emails, files and internet downloads or data stored on DTE Resources will be restricted to staff that require access to perform the roles associated with their jobs.

(51) Reports and data from internet usage monitoring may be accessed by the DTE and Information Management and Security staff to aid in responding to an investigation of a security incident. 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, web browsing and other communications

b. Reviewing logs and usage reports
c. Conducting audits and investigations

(52) In the event a formal investigation is required, Melbourne Polytechnic will initiate an internal approval process requiring 2 levels of approval:

a. Senior Leadership: CEO or Senior Executives, and
b. Director, Information Management and Security or Director ICT Services.

(53) All users of MP DTE resources must:

a. Use MP 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 their access to DTE resources is provisioned when commencing work at MP and will be removed and/or restricted immediately when they leave MP.

(54) If there is a reasonable belief that MP DTE resources are being used in breach of this policy, DTE services with guidance from the immediate manager of the person who is suspected of inappropriate use may secure the equipment while the suspected breach is being investigated.

MP Allocated Mobile Phones

(55) Mobile phones and/or mobile devices may be provided to staff members who are required to work off campus, remotely or undertake a role where immediate contact is required.

(56) The Director ICT Services will need to approve the purchase based on justification provided by the staff member's supervisor, and sign-off by their Senior Manager.

(57) General Conditions for MP provided mobile phones:

a. Corporate devices will only be allocated to staff in ongoing, full-time roles with the Institute.
b. General staff will be provided with a standardised mid-range smart phone. Advanced features will need to be justified by supervisor.
c. Any additional requirements above and beyond the standard will need to be covered at the requesting departments own cost.

(58) Your mobile device can contain confidential Melbourne Polytechnic information and access to Melbourne Polytechnic's information systems. All staff are responsible for securing mobile devices when outside of Melbourne polytechnic facilities, including, but not limited to keeping the devices in a concealed and secure location when not in the staff member's physical possession.

(59) Any potential unauthorized access to mobile devices will need to be reported to Melbourne Polytechnic DTE who will investigate the incident.

(60) Melbourne Polytechnic reserves the right to monitor device access to its information systems and device validation including, but not limited to operating system levels, patch levels, anti-malware status and database levels, and have to right to block access if any of these components are not within DTE approved specifications.

(61) All mobile devices containing or providing access to confidential data owned by Melbourne Polytechnic or for use by Melbourne Polytechnic must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, tablets, and mobile telephones.

(62) Melbourne Polytechnic mobile phones shall be managed under a Mobile Device Management (MDM) system which provides the ability to remotely locate, disable, lock and delete any data stored on the mobile phone.

(63) For additional information on the usage and management of MP allocated Mobile Devices, refer to Mobile Device Usage and Management Standard.

Bring Your Own Device (BYOD)

(64) Staff may use a personally owned device such as a laptop, tablet or smart phone to access MP Systems and Services provided the following conditions are met:

a. MP systems or services should not be accessed when using free or public Wi-Fi as information transmitted and received can be intercepted;
b. Users must not connect a personally owned device to a wired network port or via VPN to MP infrastructure without express authorisation from both the Director, Information Management and Security and Director ICT Services. Staff may connect their personal devices to the MP Wi-Fi network (SSID: wifi@MP) or remotely MP access MP services via the Internet;
c. Users must comply with this Acceptable Usage (Staff) Policy when using their personal devices to access MP systems and services;
d. Staff must not let others use their personal device which are used to access MP systems and services without their permission and supervision;
e. Staff should only use their personal charging cable and power adaptor when charging their mobile phone in public spaces as they can be infected with malware;
f. Staff should use security software and configure security features such as anti-virus / anti-malware, device encryption, enabling of phone remote tracking features (such as “Find my Phone”), auto-lock after inactivity; and
g. Staff must implement password protection (password, PIN or biometrics) for restricting access to the personal device;
h. Staff must immediately report to DTE Services in the event of a loss or theft of any device containing MP data. Where applicable, DTE Services may remotely delete all data on the lost or stolen device to ensure any sensitive or confidential MP information stored on the device cannot be accessed by unauthorised users or the public;
i. Staff must remove all data belonging to the MP on any personal owned devices before leaving the MP.

(65) To ensure the security of MP information, any personal devices accessing MP systems or information must have up to date software and applications installed to address known vulnerabilities, including the following conditions:

a. Staff turn on automatic updates and ensure software receives and applies the latest fixes.
b. Staff should only install secure and reputable apps which are downloaded from an official app store and remove apps when they are no longer required.
c. Staff must not circumvent operating system security measures designed to protect the integrity of their personal device, software and / or applications including rooting or jailbreaking devices.
d. Staff must keep internet browsers and plugins updated when accessing MP Web Application systems (systems accessed through an internet browser).

(66) Devices with known security compromises, vulnerabilities, or that can no longer receive software updates must not be used to access MP systems and information until these issues have been resolved.

(67) Staff must not store sensitive, confidential, or personal MP information on personal devices.

Removable Media

(68) To prevent risk of malware infections and loss of sensitive information, Melbourne Polytechnic will not permit the use of removable media without a valid business case and explicit approval from DTE Services and Information Management and Security.

(69) In cases where removable media is required for performance of staff duties or when providing information required by state or federal authorities, DTE will provide the removable media to be used.

(70) All removable media must be sanitised before it can be used on MP systems.

(71) Any removal media provided for use on MP DTE resources shall not be used with any external or personal devices to reduce the risk of malware contamination.

(72) Any information with a classification of OFFICIAL: Sensitive or higher (as determined by the Information Security Classification Policy and Procedure) should not be stored on external or portable drives unless explicitly approved by DTE Services and Information Management and Security with prescribed mitigating security controls including encryption implemented.

(73) All removable media is to be recorded in a Removable Media Register developed, implemented, and maintained by the Information Management and Security department.

(74) Media is to be labelled with protective marking in line with the Information Security Classification Policy and Procedure.

(75) Media is classified to the highest sensitivity or classification of information stored.

(76) Media is only used with systems that are authorized to process, store or communicate its sensitivity or classification.

(77) Any media connected to a system with higher sensitivity or classification than the media is reclassified to the higher sensitivity or classification.

(78) Before reclassifying media to a lower sensitivity or classification, or prior to disposal. The media must be sanitised, and a formal approval from the Records Services Manager be granted to reclassify and / or dispose of it.

(79) Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage.

(80) Any lost or stolen removable media must be reported to Information Management and Security as soon as possible.

(81) Removable media devices that are no longer required, or have become damaged, must be disposed of securely in accordance with Guideline – Records Destruction to avoid data leakage.

(82) Removable media devices must be returned to MP during the cessation process of staff members.

Clean Desk Policy

(83) To ensure the security and confidentiality of MP information and records all staff must maintain a clean desk when workspaces are unattended or outside of business hours. This requires all sensitive and confidential information, in electronic or hardcopy format, to be appropriately managed and stored to protect it from unauthorised access.

(84) The following steps must be followed to maintain a clean desk:

a. All sensitive and confidential documents must be placed in a drawer or filing cabinet when not in use. If this information is of a sensitive nature the drawer or filing cabinet must be locked when the information is not in use.
b. Draft documents, report statistics and figures, duplicate documents, or documents due for disposal that contain sensitive or confidential information must be placed in the designated secure disposal bins for disposal, in accordance with the Records Management Policy, and Procedure and Guidelines.
c. Computers must be locked (Windows Key + L) when unattended and shut down at the end of each workday.
d. Laptops, tablets, and other hardware devices must be removed from plain view and placed in a drawer or filing cabinet, when not in use
e. Keys for accessing drawers or filing cabinets should be stored out plain view or taken home with the staff member.
f. Passwords must not be written down in an accessible location (e.g. post-it note on desktop).
g. Any sensitive or confidential information written on whiteboards must be wiped off at the end of each day.
h. Print jobs containing sensitive and confidential paperwork should be retrieved immediately.

(85) Removable media including but not limited to CR-ROM, DVD, BlueRay and USB drives must be treated as sensitive and secured in a locked drawer when not in use by the owner.

(86) DTE Services and Records Services reserve the right undertake spot checks as well as random and scheduled audits to ensure these processes are being followed, where any breaches are identified they may be reported to your line manager.

Records Destruction and sanitisation

(87) MP – Guideline Records Destruction must be followed when decommissioning an DTE Resources containing MP information. The data purging and sanitisation process outlined in the guideline must be followed when re-using DTE Resources and where sanitisation cannot be applied records must be destroyed.

Reporting of Inappropriate Use

(88) Users who receive unsolicited offensive material from an unknown external source or a known source within MP must report it immediately to their Line Manager or Director who will determine if the Director ICT Services and/or Information Management and Security is/are to be advised.

(89) All employees, contractors, employees of any contractor, volunteers or guests of MP must immediately report any data breaches (e.g. unauthorised access, disclosure or loss of Personal Information or Sensitive Information) or suspected breaches that come to their attention in alignment with the MP Data Breach Policy.

Violation of the Policy

(90) Violations of this policy will be regarded as a serious matter and appropriate action will be taken based on the nature of inappropriate use of MP ICT resources. Violation of policy may result in

a. Suspension or revocation of IT resource access, including but not limited to: Prohibiting the staff 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 staff has committed, is committing or intends to commit misconduct.
c. In addition to any disciplinary action by MP, 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.

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

(92) Serious or repetitive misconduct may lead to disciplinary action, including the revocation of staff account or suspension during investigations or termination of employment.

(93) 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 MP management.

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

Section 4 - Accountability and Responsibility

(95) All MP Employees are responsible for:

a. Reading and acknowledging their understanding of the Acceptable Use Policy (this Policy).
b. Ensuring that their use of MP DTE resources complies with this policy.
c. Taking reasonable steps to protect Personal Information from misuse, loss and unauthorised access, modification, or disclosure.
d. Reporting and assisting in the investigation and mitigation of suspected breaches or non-compliance with this policy.

(96) Information Management and Security team (IM&S) and Digital and Tech Experience (DTE) Services are responsible:

a. Monitoring for any conduct that is non-compliant with this Policy.
b. Investigating breaches of proper use of MP DTE resources and mitigating all data breaches.
c. Granting exemptions to this Policy.
d. Ensure all DTE contract workers read and acknowledge their understanding of this Policy prior to commencing work with MP.

(97) People and Culture are responsible for:

a. Ensure all new MP staff read and acknowledge their understanding of this Policy during the induction process.

Section 5 - Definitions

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

a. Access: permissions and privileges granted to a user within a computer system or network.
b. Authentication: a process of verifying the identity of a user who is attempting to access a system or network. User presents two or more pieces of evidence (e.g Use ID, Password, Token, PIN, Biometrics) that will be validated by the system before access is granted.
c. Cloud Services: Service or resource available to MP Users or students that is hosted offsite in the cloud.
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. Copyright Material: Physical or electronic material to which only the original creators of products and anyone they give authorization to are the only ones with the exclusive right to reproduce the work.
f. Data: Information that has a value and meaning, translated into a form that can easily be transferred or processed.
g. Data Breach: Unauthorised access, disclosure or loss of any Personal Information or Sensitive Information held by MP.
h. Denial of Service (DoS): an interruption in an authorised user's access to a computer network, web page, system or application, typically one caused with malicious intent.
i. Disruption of Network Communication: includes, but is not limited to network sniffing, ping floods, packet spoofing, denial of service, key logging, and forged authentication and routing information for malicious purposes.
j. Hacking: any act of gaining unauthorized access to computer systems, networks, or data.
k. 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 work use.
l. Malicious Software: any malicious program that causes harm to a computer system or network. Malicious Malware Software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware or rootkits.
m. Network Monitoring: any inspection of data across the network in real time. It is used for network management but can also be used by malicious users to covertly inspect or intercept data not intended for their workstation.
n. Network Penetration test: a process of assessing the security of a computer network by simulating attacks from malicious outsiders (or insiders) to identify vulnerabilities that could be exploited by unauthorized individuals or entities.
o. Password: A sequence of characters used for authentication.
p. Personal Information: means information or an opinion (whether true or not) about an individual whose identity can reasonably be ascertained and can include names; signatures; tax file numbers; postal and email addresses; phone numbers; and information or opinions about health issues or a disability, race, ethnicity, religion, political opinion, sexuality or criminal record.
q. Plagiarism: Plagiarism is the act of using someone else's work, ideas, or intellectual property without proper attribution or permission and presenting it as one's own.
r. Phishing: a type of cyber-attack in which attackers use deceptive techniques, typically via email, messaging platforms, or websites, to trick individuals into providing sensitive information such as login credentials, personal information, or financial details.
s. Port Scanning: a technique used to discover open ports and services running on a target system or network that could be used to identify security vulnerabilities and compromise a system.
t. Proxy Avoidance: techniques used to bypass or circumvent restrictions imposed by MP proxy servers or content filtering systems. Proxy servers are intermediary servers that act as an intermediary between a user's device and the interne
u. Record: Any information created or received by a staff member as part of their daily work for Melbourne Polytechnic. Records can include documents, email, spreadsheets, photographs, audio visual materials, official social media posts, databases, etc.
v. Removable Media: A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).
w. Sensitive Information: all data, in its original and duplicate form, for which there is either a legal, ethical, or contractual requirement to restrict access. Examples include financial information, system access passwords, building plans, tenders and contracts, information about a third party with whom MP has a commercial relationship, etc.

x. SPAM: Irrelevant or unsolicited messages sent over the internet, typically to many users, for the purposes of advertising, phishing, spreading malware, etc.

y. Users: MP MP's employees, contractors, employees of any contractors, volunteers and guests that has access to MP network or systems.

z. Web Filter Categories: Categories of websites or web pages that have been assigned based on their dominant Web content. A website or webpage is categorized into a specific category that is likely to be blocked according to its content.

Status and Details

Status	Current
Effective Date	3rd January 2025
Review Date	14th May 2029
Approval Authority	Executive Director Finance, Reporting, Assurance and Marketing
Approval Date	18th December 2024
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