Video Conferencing Policy

Section 1 - Purpose

(1) This policy sets out the requirements for use of Video Conferencing (VC) solutions at Melbourne Polytechnic (MP).

(2) The Video Conferencing Guideline set out in Schedule A provides Zoom meeting hosts with advice on how to secure Zoom meetings to prevent unwanted guests and disruptions.

Section 2 - Principles

(3) This policy is guided by the following principles, standards, acts & legislation:

a. Melbourne Polytechnic's Strategic Vision & Values
b. Users and students will have access to VC resources needed to perform their duties and carry out their studies
c. Users and students will use VC systems in a lawful manner, in line with Melbourne Polytechnic's Code of Conduct Policy and Student Code of Conduct Guidelines.
d. Users and students conduct themselves and their use of VC Systems in and ethical and responsible manner.

Section 3 - Breach of this Policy

(4) Where Melbourne Polytechnic suspects or finds evidence of a breach of this policy, Melbourne Polytechnic may take action including but not limited to, any or all of the following:

a. Removal/restriction of access to Melbourne Polytechnic Video Conferencing systems
b. Taking disciplinary action against a student in accordance with the Student Discipline Policy
c. Taking disciplinary action against employees in accordance with relevant Agreement and/or Code of Conduct Policy, and OHS/anti-discrimination policies
d. Notifying federal or Victorian authorities, regulators and/or insurers including law enforcement bodies
e. Taking legal action under applicable civil or criminal laws.

(5) Any User or student authenticating into any MP Video Conferencing Solution will be assumed to understand and agree with this policy.

Section 4 - Scope

(6) This policy applies to anyone who uses Melbourne Polytechnic VC solutions including Board and Committee members, employees, contractors, employees of any contractors, volunteers, visitors, guests, and students.

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the Policy and Procedure Register for the latest version.

Section 5 - Video Conferencing

(7) Video Conferencing solutions are provided for Melbourne Polytechnic educational and business purposes only. These facilities are available to users and students of Melbourne Polytechnic. Any use of these video conferencing services outside of “MP approved activities” is strictly prohibited.

Section 6 - Guiding Principles for Video Conference Participants:

(8) Anyone participating in a video conference must be positioned so he or she cannot be easily overheard or overlooked.

(9) If the room has windows looking out onto other work areas, ensure video cameras are not positioned where they could inadvertently film sensitive documents or computer screens on surrounding desks, or microphones pick up sensitive conversations taking place nearby.

(10) In instances where video conferencing is conducted directly from users’ or students’ desks, then cameras must be positioned to focus solely on the individual, and the sensitivity of the microphone should be tuned to a minimum to reduce the risk of other conference participants seeing or hearing something inappropriate.

(11) Cameras and microphones should be disabled when not in use, either by disconnecting the power, connection cables or using lens caps.

(12) Due to the widespread abuse of video conferencing installation files to spread viruses, any installation on managed Melbourne Polytechnic Standard Operating Environment (SOE) devices must be through the software catalogue, any installation on non-managed devices must be through the official websites for Zoom or Microsoft Teams, or through the Apple and Android stores for mobile devices (including tablets)

(13) Where the Zoom client is installed on a personal device the user or student must ensure the latest version of the Zoom client is installed through updates and patching. This ensures that the latest features of the Zoom platform will be supported and that any known vulnerabilities have been addressed.

(14) Due to the prevalence of Zoombombing attacks, meeting invites and passwords must not be forwarded to anyone other than the explicit meeting invitees. This includes through email, posting a link on social media, online communications platforms, online forums or through any other electronic format.

Section 7 - Prohibited Conduct

(15) Video Conferencing Services must not be used:

a. For any illegal or fraudulent purpose
b. In a way that endangers a person or damages property
c. To display or transmit material that is obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an email or in an attachment to an email, or through a link to an internet site (URL).
d. In any way that causes insult, offence, intimidation or humiliation by reason of unlawful harassment or discrimination
e. To commit an offence

f. To communicate, transmit or distribute any computer worms, trojans, viruses, or other similar programs
g. To send unsolicited electronic messages, links, images or files
h. To distribute or publish any content in contravention of applicable law or regulation
i. To do anything which might compromise the security or safety of, or which might damage, interrupt or interfere with the operation of the Service
j. To violate a law or cause Melbourne Polytechnic to violate a law

(16) It is expressly prohibited for any user or student to:

a. Record a Video Conferencing session through any means without the explicit consent of all participants
b. Authenticate to MPs video conference systems using another User's or student's credentials
c. Exploit any vulnerabilities in Video Conferencing Systems that can compromise the security or safety of, or which might damage, interrupt or interfere with the operation of the Service.

Section 8 - Recording of Video Conferencing Sessions

(17) Meetings and online classes may be recorded for reference purposes. When this occurs the users or students will be provided with the following disclaimer when joining the session, for which they will need to consent to stay in the session or leave.

> "By attending this lecture/meeting, you are consenting to your face/voice/content being recorded. If you leave the lecture/meeting you must make alternative arrangements for completing coursework/assessments. Recorded lectures/meetings are stored in the cloud on Zoom servers in Australia and uploaded to Moodle. See Melbourne Polytechnic's, Zoom's and Moodle's websites for their privacy policies."

Section 9 - Mandatory wording for Zoom invitations

(18) When scheduling a Zoom meeting the following text will be globally configured for the invitation:

> "You must not share or forward this Zoom invitation or link to anyone else. It is for you only. Sharing or forwarding this Zoom invitation may cause an unauthorised person to access Zoom and use it inappropriately."
>
> "Please be aware that cyber criminals may send you Zoom invitations that could cause viruses if you click on the link. If you are unsure whether a Zoom invitation is genuine, please contact the meeting organiser."

Section 10 - Mandatory wording for Zoom Waiting Room Messages

(19) By default MP uses the Waiting Room feature to control which participants can enter a Zoom Video Conferencing Session. While participants are waiting to be admitted into a meeting room they are presented with a message. This provides an opportunity to display a disclaimer around the Video Conferencing Policy to all Users and students, to ensure that they understand their obligation to read and abide by the policy.

(20) The following message is configured in the Global Settings for all MP Zoom Video Conferencing Sessions. Note that a character limit of 400 characters applies to this message.

> You are currently waiting to join an MP Video Conference Session. Please note that by authenticating into this VC session it will be assumed that you have read and agreed with the following Video Conferencing Policy:

Section 11 - Who to notify if a “Zoombombing” attack occurs?

(21) A zoombombing attack can be quite confronting, however in order to enable Melbourne Polytechnic to appropriately investigate the attack some details around the incident will be need to be provided. Users will need to gather evidence around the attack such as time of attack, the details of the perpetrator and the nature of the attack, and a list of the persons who were exposed to the attack. These details are to be reported to the service desk (03) 9269 1455 (who will create a ticket on behalf of the user) or through the staff service portal on the intranet by raising a ticket under “IT Security” and then “Incident”. The incident will then be classified, investigated and actioned based on the Melbourne Polytechnic Incident Response Policy.

Section 12 - Monitoring – Video Conferencing Details

(22) Melbourne Polytechnic does not generally access or monitor individual Video Conferencing sessions but it does analyse the statistics across all Video Conferencing sessions for capacity planning.

(23) However, Melbourne Polytechnic reserves the right to access and monitor Video Conferencing Sessions for any reason, including suspected breaches of this policy by users or students, or suspected unlawful activities.

(24) Access to and monitoring includes, session logs, participant lists and details. DTE may keep a record of any monitoring for investigative purposes.

(25) When an investigation is requested in relation to an incident, Melbourne Polytechnic will initiate the following internal approval process based on who requested the investigation and if there is a potential for conflict of interest:

a. If the Chief Executive (CE) requests the investigation then it does not need to be approved/endorsed by anyone else
b. If an Executive Director requests an investigation then the CE should be informed, unless it involves the CE and then the Director Enterprise Risk and Compliance should be informed

(26) The requester will then nominate an independent incident owner who will be responsible for:

a. Determining a course of action to appropriately address the incident, within their delegation, and escalation where an appropriate response is outside of the incident owners delegation.
b. Reporting of progress and any issues faced to appropriate levels of management based on the incident type and impact.

(27) In the event that a potential conflict of interests exists, this incident owner should be nominated from outside of the areas under investigation, or should be sourced from outside of the organisation where the appropriate expertise and independence does not exist internally. Staff who are involved the investigation must adhere to Melbourne

Polytechnic's Code of Conduct Policy at all times.

Section 13 - Definitions

(28) Cloud Services: Service or resource available to Melbourne Polytechnic Users or students that is hosted offsite in the cloud.

(29) IT Resource: All physical assets, software, applications and services provided, maintained or managed by DTE.

(30) Malicious Software: Refers to 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.

(31) Microsoft Teams: Is cloud-based team collaboration software that is part of the Office 365 suite of applications. The core capabilities in Microsoft Teams include business messaging, calling, video meetings and file sharing. Businesses of all sizes can use Teams.

(32) Sensitive Information: all data, in its original and duplicate form, for which there is a commercial, legal, ethical, or contractual requirement to restrict access. For example: financial information, system access passwords, building plans, tenders and contracts, information about a third party with whom Melbourne Polytechnic has a commercial relationship, etc. Sensitive information must be restricted to those with a legitimate business need for access.

(33) Standard Operating Environment (SOE): Is a standard implementation of an operating system, updates, patches and associated software. It is typically implemented as a standard disk image for mass deployment to multiple computers in an organisation to ensure ease of deployment and consistency of software across the organisation.

(34) URL: A Uniform Resource Locator (URL), also known as a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

(35) User: Melbourne Polytechnic's employees, contractors, employees of any contractors, volunteers and guests.

(36) Video Conferencing: Videoconferencing (or video conference) means to conduct a conference between two or more participants at different locations by using computer networks to transmit audio and video data.

(37) Vulnerability: In computer security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system.

(38) Waiting Room: The Waiting Room feature in Zoom allows the meeting host to control when a participant joins the meeting. It is a virtual staging area where participants wait to be admitted by the meeting host.

(39) Zoom: Is a web-based video conferencing tool with a local, desktop client and a mobile app that allows users to meet online, with or without video.

(40) Zoom Client: Is a software application that can be installed and provides a user with accesses to the Zoom Video Conferencing platform through the internet.

(41) Zoom Cloud: The Zoom cloud is a proprietary global network that hosts the Zoom Services including storage of recorded Zoom Video Conferencing Sessions.

(42) Zoom Invitation: A Zoom Invitation is an electronic request to attend a Video Conferencing Session often sent over email with a URL link to the session.

(43) Zoombombing: is where an unwanted intrusion into a Zoom Video Conferencing Session occurs that causes a

disruption such as posting or presenting lewd or inappropriate content.

Section 14 - Responsibility and Accountability

Task	Responsibility	Notes
Monitor for any conduct that is non-compliant with this policy	DTE Services	
Classify, investigate and action any reporting “Zoom bombing” incidents including informing the relevant internal and external authorities depending on the nature and severity of the incident.	DTE Security & Legal Counsel	
Assess and instigate disciplinary actions against any staff found to be in breach of this policy	Representative from People and Culture at Director level	
Investigate potential student breaches of Melbourne Polytechnic Video Conferencing policy and systems.	Director ICT Services (CIO)	Potential student breaches of the video conferening policy will be addressed under Melbourne Polytechnic's Student Discipline Policy. Investigations will take place in conjunction with relevant teaching and non teaching staff.
Adhere with the video conferencing principles in this policy.	All Users	

Section 15 - Supporting Documents and Templates

(44) Melbourne Polytechnic Policies and Procedures

a. Code of Conduct Policy
b. Delegation of Authority Policy
c. Employee Grievances Policy
d. Equal Opportunity, Discrimination and Harassment Policy
e. Information Technology Resources (All Users) Policy
f. Information Technology Usage (Students) Policy
g. Managing Personal Information and Sensitive Information Guideline
h. Health, Safety and Wellbeing Policy
i. Personal Information Management Policy
j. Bullying Prevention and Management Policy
k. Prospective Employees and Employees Privacy Policy
l. Records Management Policy
m. Records Management Procedure
n. Social Media Policy
o. Student Code of Conduct Guidelines
p. Student Complaints and Appeals Procedures
q. Student Discipline Policy
r. Student Equal Opportunity, Discrimination and Harassment Policy
s. Health and Safety Manual.

(45) Legislation

a. Copyright Act 1968 (Cth)
b. Disability Discrimination Act 1992 (Cth)
c. Equal Opportunity Act 2010 (Vic).
d. Racial and Religious Tolerance Act 2001 (Vic)
e. Fair Work Act 2009 (Cth)
f. Health Records Act 2001 (Vic)
g. Privacy Act 1988 (Cth)
h. Privacy and Data Protection Act 2014 (Vic)
i. Racial Discrimination Act 1975 (Cth)
j. Sex Discrimination Act 1984 (Cth)
k. Trade Marks Act 1995 (Cth)
l. Competition and Consumer Act 2010 (Cth)
m. Victorian Protective Data Security Framework,

Status and Details

Status	Current
Effective Date	7th July 2020
Review Date	7th July 2025
Approval Authority	Executive Leadership Committee
Approval Date	7th July 2020
Expiry Date	Not Applicable
Policy Owner	Joseph Santiago Executive Director Finance, Reporting, Assurance and Marketing
Policy Implementation Officer	Channa Jayasinha Director ICT Services
Author	Channa Jayasinha Director ICT Services
Enquiries Contact	Channa Jayasinha Director ICT Services

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the Policy and Procedure Register for the latest version.