Mobile Devices Usage and Management Standard

SECTION 1 - PURPOSE

(1) Mobile Devices are important tools for Melbourne Polytechnic and their use is supported by the institute to achieve its goals. While their portability makes these devices useful, they may also introduce issues due to risks associated with greater exposure to external threat actors, inappropriate use and security of the information being transmitted and/or stored on these devices.

(2) This Standard is part of Melbourne Polytechnic's Information Security policy suite and complying with the standard will ensure that consistent and appropriate controls are applied to the Institute's owned mobile devices to help mitigate the risks associated with their use.

(3) This Standard aims to:

a) Ensure that Melbourne Polytechnic data on mobile devices is properly protected from unauthorised access, dissemination, alteration or deletion.

b) Ensure the use of Mobile devices at Melbourne Polytechnic aligns with the relevant security requirements and industry best practices.

c) Reduce information security risks below associated with uses of Mobile devices:

i. Device Loss - Devices used to transfer or transport work files that could be lost or stolen.

ii. Data Theft - Sensitive corporate data is deliberately stolen and sold by an employee or unsanctioned third party

iii. Copyright - Software copied onto a mobile device could violate licensing.

iv. Malware - Viruses, Trojans, worms, spyware, malware, and other threats could be introduced via a mobile device.

v. Compliance - Loss or theft of financial and/or personal and confidential data could expose Melbourne Polytechnic to the risk of non-compliance with Australian data privacy laws.

vi. Exposure of MP Systems – Compromise of a mobile device could lead to further access to MP internal systems and information by a threat actor

SECTION 2 - SCOPE

(4) This standard applies to all MP staff, contractors and third parties that that have been issued with a Melbourne Polytechnic owned mobile device (such as laptops, mobile phones/smartphones and tablets).

(5) The Standard applies to the use of mobile devices regardless of location, both during and outside of office hours.

(6) For this Standard, Mobile Devices refers to all devices and accompanying media that fit the following categories:

a) Smartphones, tablets or any other mobile/cellular phones

b) e-readers

c) portable media devices

d) portable gaming devices

e) laptop/notebook/ultrabook computers

f) personal digital assistants (e.g. PDAs)

g) any other mobile device capable of storing corporate data and connecting to a network.

(7) Personally owned devices are out of scope of this Standard. See the Bring Your Own Device (BYOD) section in the MP Acceptable Usage (Staff) Policy for information on the use of personally owned devices to process Melbourne Polytechnic data.

SECTION 3 - STANDARD

Standard Statement

(8) MP is committed to protecting its information assets against security events or incidents that could impact the confidentiality, integrity and availability (CIA) of MP information.

(9) MP conducts its business activities in compliance with relevant data protection laws and regulations, including but not limited to, ACSC's Information Security Manual (ISM), Privacy and Data Protection Act 2014 (Vic), Victorian Protective Data Security Framework (VPDSF), Public Records Act 1973 (Vic), and the Privacy Act 1988 (Cth).

(10) Connectivity and configuration of all mobile devices will be centrally managed by the ICT Services to ensure compliance with this standard.

Standard Principles

(11) This Standard will be guided by the following principles, standards, acts & regulations:

a) MP's Strategic Vision & Values
b) Victorian Protective Data Security Standards (VPDSS 2.0)
c) Information Privacy Principles (IPPs) which is a requirement for all Victorian Government Agencies under the Privacy and Data Protection Act 2014 (PDP Act)
d) Australian Cyber Security Centre (ACSC) Essential 8
e) The Australian Government Information Security Manual (ISM), specifically the Event Logging and Monitoring section under the Guidelines for System Monitoring
f) National Institute of Standards and Technology (NIST) Special Publication 800-92 (Revision 1 - 2023).
g) Public Records At 1973 (Vic) and Public Record Office Victoria (PROV) Standards

Standard Topics

Mobile Devices usage

(12) All mobile devices must be protected by a strong password or pin code to prevent unauthorised use. Passwords and pin codes must not be written down, stored with the mobile device or disclosed to other persons. For further information, refer to the MP Authentication Policy.

(13) All users of mobile devices must employ reasonable physical security measures to protect their mobile device when in use, when travelling with the device, or when it is unattended.

(14) In the event a mobile device is lost or stolen, the user must notify the Melbourne Polytechnic ICT Services immediately.

All users must follow the following principles as recommended in the Australian Government's Information Security Manual (ISM) requirements:

	Topic	Requirement
(15)	Personnel awareness	i. Personnel must understand the sensitivity or classification permitted for voice and data communications when using mobile devices. Where Personnel are not sure, guidance should be sort from their people leaders or Information Management and Security (IM&S) team
		ii. Personnel must take the following precautions when using mobile devices:

		• never leave mobile devices or removable media unattended, including by placing them in checked-in luggage or leaving them in hotel safes • never store credentials (passwords, tokens, etc.) with mobile devices that they grant access to, such as in laptop computer bags • never lend mobile devices or removable media to untrusted people, even if briefly • never allow untrusted people to connect their mobile devices or removable media to your mobile devices, including for charging • never connect mobile devices to designated charging stations or wall outlet charging ports • never use gifted or unauthorised peripherals, chargers or removable media with mobile devices • never use removable media for data transfers or backups that have not been checked for malicious code beforehand • avoid reuse of removable media once used with other parties' systems or mobile devices • avoid connecting mobile devices to open or untrusted Wi-Fi networks • consider disabling any communications capabilities of mobile devices when not in use, such as Wi-Fi, Bluetooth, Near Field Communication and ultra-wideband • consider periodically rebooting mobile devices • consider using a VPN connection to encrypt all cellular and wireless communications • consider using encrypted email or messaging apps for all communications.
(16)	Using paging, message services and messaging apps	Paging, Multimedia Message Service, Short Message Service and messaging apps must not be used to communicate sensitive or classified data.
(17)	Using mobile devices in public spaces	i. Sensitive or classified data must not be viewed or communicated in public locations unless care is taken to reduce the chance of the screen of a mobile device being observed.
		ii. Sensitive or classified phone calls must not be conducted in public locations unless care is taken to reduce the chance of conversations being overheard.
(18)	Maintaining control of mobile devices	i. Mobile devices must be kept under continual direct supervision when being actively used.
		ii. Mobile devices must be carried or stored in a secured state (locked) when not being actively used.
		iii. If unable to carry or store mobile devices in a secured state, they must be physically transferred in a security briefcase or an approved multi-use satchel, pouch or transit bag.
(19)	Before travelling overseas with mobile devices	i. Personnel must understand the privacy and security risks when travelling overseas with mobile devices. Where Personnel are not sure, guidance should be sort from their people leaders or Information Management and Security (IM&S).
		ii. Before travelling overseas with mobile devices, personnel must take the following actions: • record all details of the mobile devices being taken, such as product types, serial numbers and International Mobile Equipment Identity numbers

		• update all operating systems and applications • remove all non-essential data, applications and accounts • backup all remaining data, applications and settings.
(20)	While travelling overseas with mobile devices	Personnel must report the potential compromise of mobile devices, removable media or credentials as soon as possible, especially if they: • provide credentials to foreign government officials • decrypt mobile devices for foreign government officials • have mobile devices taken out of sight by foreign government officials • have mobile devices or removable media stolen, including if later returned • lose mobile devices or removable media, including if later found • observe unusual behaviour of mobile devices.
(21)	After travelling overseas with mobile devices	Upon returning from travelling overseas with mobile devices, personnel must take the following actions: • sanitise and reset mobile devices, including all removable media • decommission any credentials that left their possession during their travel • report if significant doubt exists as to the integrity of any mobile devices or removable media.

Mobile Device Management

(22) ICT Services must use a mobile device management (MDM) solution to secure devices and enforce policies remotely. Before connecting a mobile device to corporate resources, the device will be automatically enrolled prior to being issued to the user. The MDM must support the following:

- remote wipe information stored on the devices when required.
- enforcement of security policies, including mandating the use of a PIN to secure the device
- location tracking if the device is lost or stolen.
- application deployment and visibility.
- hardware feature management.

Mobile Devices System administrators must follow the following principles as recommended in the Australian Government's Information Security Manual (ISM) requirements:

	Topic	Requirement
(23)	Mobile device management policy	Mobile Device Management solutions that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Management, version 4.0 or later, must be used to enforce mobile device management policy.
(24)	Mobile device management policy	Mobile devices that can access OFFICIAL: Sensitive or PROTECTED systems or data must use mobile platforms that have completed a Common Criteria evaluation against the Protection Profile for Mobile Device Fundamentals, version 3.3 or later, and are operated in accordance with the latest version of their associated ASD security configuration guide.
(25)	Data storage	Mobile devices must encrypt their internal storage and any removable media.
(26)	Data communications	Mobile devices must encrypt all sensitive or classified data communicated over public network infrastructure.
(27)	Maintaining mobile device security	i. Mobile devices must be configured to operate in a supervised (or equivalent) mode.

		ii.	Mobile devices must be configured with remote locate and wipe functionality.
		iii.	Mobile devices must be configured with secure lock screens.
		iv.	Mobile devices must prevent personnel from installing non-approved applications once provisioned.
		v.	Mobile devices must prevent personnel from disabling or modifying security functionality once provisioned.
		vi.	Security updates must be applied to mobile devices as soon as they become available.

Compliance to Standard

(28) Any attempt to contravene or bypass the mobile device usage requirements outlined in this standard or against the MP Acceptable Usage Policy may result in immediate disconnection from Melbourne Polytechnic resources and repossession of the devices.

SECTION 4 - RESPONSIBILITY AND ACCOUNTABILITY

(1) The Director Information Management & Security is responsible for:

a. Overseeing the governance around the Mobile Devices usage
b. Ensure Mobile Devices Standard and related processes are incorporated into other related business processes such as Information Security Incident Response.

(2) The Information Management and Security (IM&S) team is responsible for:

a) Developing and maintaining the Mobile Devices Standard in line with relevant security obligations and requirements.
b) Ensuring relevant MP stakeholders are aware of the standard and understand their roles and responsibilities in relation to logging and monitoring of events on their systems.
c) Ensuring adherence to the Mobile Devices Standard by relevant system owners and administrators responsible for managing mobile devices and report any non-compliances.

(3) Director Information and Communications Technology is responsible for:

a) Ensuring ICT team understand and incorporates the Mobile Devices Standard into their day-to-day ICT operations, and administration of Mobile Devices.

(4) ICT administrators are responsible for:

a) Configuring Mobile Devices in line with the requirements of this standard, reference to “Mobile Devices Management” section.
b) Identifying the changes needed to Mobile Devices configurations and related Mobile Device Management systems, and ensure changes are applied in line with relevant MP procedures.
c) Testing and implementation or deployment of security updates to the Mobile Devices and related Mobile Device Management systems.
d) Identifying and reporting on non-compliances to this standard.

(5) All MP staff, contractors and third parties allocated Mobile Devices are responsible for:

a) adhering to the principles prescribed in this standard

SECTION 5 - SUPPORTING DOCUMENTS AND TEMPLATES

(2) Related MP policies and procedures:

a) Information Security Policy
b) Acceptable Usage (Students) Policy
c) Acceptable Usage (Staff) Policy
d) Business Continuity Plan
e) Business Resiliency Policy
f) Code of Conduct
g) Compliance Management Procedure
h) Data Breach Response Plan
i) Disaster Recovery Plan
j) Information Security Incident Response Plan
k) Information Security Incident Response Playbooks
l) Information Security Awareness Policy
m) Privacy Policy
n) Privacy Impact Assessment Procedure
o) Records Management Policy
p) Records Management Procedure
q) Risk and Compliance Policy
r) Risk Management Framework
s) Student Code of Conduct Guidelines
t) Student Discipline Policy
u) Third-Party Information Security Risk Procedure

(3) Related Legislation and Regulation

a) Higher Education Standards Framework (Threshold Standards) 2021
b) Privacy Act 1988 (Cth)
c) Privacy and Data Protection Act 2014 (Vic)
d) Victorian Protective Data Security Framework (VPDSF) Business Impact Level (BIL) Table v2.0
e) Victorian Protective Data Security Standard (VPDSS v2.0)

SECTION 6 - DEFINITIONS

(4) For the purpose of this Standard the following definitions apply:

a) Confidential Information - Sensitive personally identifiable information that must be safeguarded in order to protect the privacy of individuals and the security and integrity of systems and to guard against fraud. Note that this does not include any publicly available information that has lawfully been made available to the general public. Additionally, proprietary information, data, information, or intellectual property, in which MP has an exclusive legal interest or ownership right may also be considered confidential information.

b) Confidentiality - The property that data or information is not made available or disclosed to unauthorised persons or processes.

c) Data Breach - A data breach happens when personal information is accessed, disclosed without authorisation, or is lost.

d) Denial of Service (DoS) - A disruption in authorised user's access to systems, typically caused with malicious intent.

e) Incident Response Plan - Is the guidebook to handling information security incidents. It provides instructions around the various stages of an information security incident response including identifying stakeholders and their roles and responsibilities.

f) Information System - A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.

g) Integrity - Protection against unauthorised information modification or destruction of information

h) Isolated Device – Restricting a device access to resources and other infrastructure to contain malicious software from executing potentially harmful actions or contaminating other devices.

i) Network - a group of interconnected nodes or computing devices that exchange data and resources with each other.

j) Security Incident - Any security event that negatively impacts the confidentiality, integrity, and/or availability (CIA) of information, information systems and network infrastructure at an organisation in a way that impacts the business.

k) Third-Party - a person or company that provides services to or on behalf of the organisation.

(3) STANDARD CONTROL

Include in this section all information required, prior to submitting for approval, excluding the date approved, promulgated and the review date which will be added after approval by the Standard Office.

Approving authority	Executive Director Finance, Reporting, Assurance and Marketing
Date approved	
Date promulgated	
Standard owner	*Director Information Management and Security*
Standard implementation officer	*Director Information Management and Security*
Standard category	*Information Communication and Technology*
Edition	*1*
Review date	

(4) VERSION HISTORY

Include in this section all information required for the new/updated edition, prior to submitting for approval. DO NOT delete any information relating to previous editions.

Edition	Approved by	Approval Date	Summary of changes/Notes
1	ED FRAM		*New Mobile Devices Usage and Management Standard to demonstrate MP aligns with state and federal government standards*