Student BYOD Policy

Policy number: IS15

Version: 1.0

Policy Owner: General Manager Corporate Services

Subject Expert: Director Information Services (CIO)

Next review date: 31/5/2024

1. PURPOSE

The student BYOD Policy (this Policy) establishes the guidelines that govern all aspects for the support and responsible use of personal mobile devices utilised by South Metropolitan TAFE students. Including student satisfaction by support of personal equipment on campus grounds.

2. SCOPE

This policy applies to all students of SMT. They are responsible for exercising good judgement regarding appropriate use of information, electronic devices and network resources in accordance with the SMT policies and standards and local laws and regulations.

3. POLICY GOVERNANCE

- TS01 South Metropolitan TAFE Student Code of Conduct.
- The Western Australian Whole of Government Digital Security Policy 2016 - OGCIO
- AS NZS ISO IEC 27001 – 2006 Information technology – security techniques- information security management.
- AS NZS ISO IEC 27002 – 2006 Information technology – security techniques- code of practice for information security.
- AS NZS ISO 31000:2009 – Risk management principles and guidelines.
- Privacy Act 1988
    - Australian Privacy Principles.
    - Privacy Amendment (Notifiable Data Breaches) Act 2017

4. KEY TERMS

BYOD (Bring Your Own Device) this refers to any student bringing their own personal device on to campus to use at the facilities.

PMD (Personal Mobile Device) is a non-corporate owned device procured and owned by the student. These personal devices can include laptops, MacBooks, netbooks, tablet PC's, smartphones (Blackberry, iPhone, Android, Windows) or tablet devices (e.g. Playbook, iPad, Android) – hereby known as Personal Mobile Devices.

MDM (Mobile Device Management) is a software suite that provides mobile device management, auditing and reporting against corporate owned devices and personal mobile devices that utilise the BYOD program.

PSD (Portable Storage Device) Includes but is not limited to flash storage (e.g. USB drives, memory cards), external hard drives, portable media devices (e.g. iPod), and internal hard drives in portable computers.

Data Plan is a plan established with a provider (e.g. Telstra) for the provision of voice and or data telecommunication services.

Data Cap refers to the included data download allowance associated with a Data Plan, usually period based (e.g. 6GB per month).

Data Push is a service where SMT corporate data (email / files) are synchronised to a Mobile Device. This is typically achieved through an email server or Mobile Device Management software suite.

App or Apps refers to small application programs developed specifically for mobile devices which may be free or commercially available (e.g. iTunes or Google Play Store).

Authorised User - is an authorised person who uses a computer or network service. A user has a user account and is identified by a username.

Data - information, in any form, (including emails) on which computer programs operate. Can be stored within networks or computing facilities or on devices which may be connected to networks.

Password - is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource (example: an access code is a type of password). The password should be kept secret from those not allowed access.

Student – is an enrolled learner.

User Account - allows a user to authenticate to system services and be granted authorisation to access them; however, authentication does not imply authorisation. To log in to an account, a user is typically required to authenticate oneself with a username and password or other credentials for the purposes of accounting, security, logging, and resource management.

MFA – Multi Factor Authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

5. PRINCIPLES

5.1 Bring Your Own Device (BYOD)

5.1.1 Context

Personal devices can be connected to the SMT GUEST Wi-Fi network. Students are responsible for the protection and upkeep of their own equipment and software, and safeguarding the use of their accounts.

` Students who connect a PMD up to the SMT GUEST Wi-Fi network accept the terms of this policy.

5.1.2 Data Responsibility / Backups

SMT is not responsible for the backup or recovery of data on any Personal Mobile devices (PMD) used within the BYOD framework. The responsibility for any personal data remains with the student. If required to delete TAFE data from a PMD, SMT will not compensate for that loss of data. SMT will not install any application software (e.g. iTunes) on TAFE assets for the purpose of backing up PMD data.

5.1.3 SMT Device Control

SMT reserves the right to remove any student from the BYOD program.

5.1.4 Data Privacy

SMT's data is restricted to designated ICT personnel for audit, support and compliance. Data from this system can only be utilised by approval from the CEO, General Manager Corporate Services or Director of People and Culture.

5.1.5 Legal

Students who utilise the BYOD must be aware that in the case of legal action or police investigations PMD's may be confiscated because of an enquiry or criminal investigation as per the external authorities' processes.

5.1.6 PMD Lost, Broken or stolen devices

SMT is not responsible for any damages, insurance, theft, or loss of PMD on its campuses. Any loss or damage to personal devices is the students' responsibility, and suitable insurance or protection is the responsibility of the user.

5.1.7 PMD Device Costs

Personal Device usage, and all associated costs and charges are the responsibility of the student. SMT is not responsible for any associated costs of a student's PMD. This includes but is not limited to any insurance, damages, warranty, legal, data plans, exceeding data caps, PSD memory, accessories & peripherals.

5.1.8 Best Effort Support Model

SMT ICT will provide a "Best Effort Support Model" regarding student PMD's. Best effort is defined as SMT providing reasonable remote assistance supporting students. Under the support model the following services are supported:

* Troubleshooting for wireless connectivity to the SMT GUEST Wi-Fi network.

All other support and application issues with a PMD remain the responsibility of the student using a PMD.

5.1.9 Application Costs

SMT will not pay for or reimburse any application costs for a PMD device. SMT is under no obligation to cover the application costs as the program is voluntary. This includes email clients.

6. DOCUMENTS SUPPORTING THIS POLICY

6.1. **Policies**

- TS01 South Metropolitan TAFE Student Code of Conduct
- IS01 Student Acceptable Use Policy
    - IS08 ICT Access Control Policy
    - IS04 ICT Information Security Policy

6.2. **Procedures**

6.3. **Forms**

6.4. **Other**

7. POLICY REVIEW AND COMMUNICATION

All students can review relevant copies of these policies via the student hub.

8. POLICY APPROVAL

Approved and Endorsed:

Terry Durant

Managing Director

Date: 6/6/2023

9. DOCUMENT HISTORY AND VERSION CONTROL

Version	Date Approved	Approved by	Brief Description
V1	6/6/2023	Managing Director	Policy Creation