# Student Acceptable Use Policy

**Policy number: IS14**

**Version: 1.0**

**Policy Owner: General Manager Corporate Services**

**Subject Expert: Director Information Services (CIO)**

**Next review date: 31/5/2024**

## 1. PURPOSE

All students using the South Metropolitan TAFE (SMT) Information Technology (IT) services are required to comply with the principles outlined in this policy. In using IT Services, all students have a right to be treated fairly and have an obligation to act responsibly. Inappropriate use exposes SMT and the Student to various risks including but not limited to malicious attacks, malware, and compromise of network and computer systems leading to reputational or legal ramifications.

## 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 South Metropolitan TAFE 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).

# 5. PRINCIPLES

## 5.1. User Acceptance & Agreement

### 5.1.1 Acceptance of South Metropolitan TAFE Acceptable Use Policy (AUP's)

Acceptance of this policy is also acceptance of the wider framework of South Metropolitan TAFE Information Communications Technology (ICT) AUP's. Training  IT assets and services are made available to students for education and training purposes. Limited personal use is permitted provided it does not impact on training delivery. They are not to be used for commercial purposes.

**5.1.2 Protect SMT interests** IT services should not be used in a way that could cause the organisation embarrassment or loss, or to promote interests other than those of the SMT.

### 5.1.3 Approved components

Only authorised equipment, software, and services can be introduced and used in SMT's environment. Personal devices can be connected to 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.

### 5.1.4 Lawful use

IT assets and resources can only be used for lawful activities, and cannot be used for any activities which would contravene any laws or regulations with which SMT is obliged to comply.

### 5.1.5 Report Issues

If you believe or suspect that something is not secure, or you need advice please promptly inform your lecturer or other SMT staff member, who will report the issue to the IT Service Desk.

## 6. Unacceptable uses of IT service

Unacceptable uses of IT services include, but are not limited to the following. Students must not:

a. use another student's digital identity, nor must you attempt to find out the password of another student, allow another person to use your digital identity, share passwords or leave your device unsecured.

b. attempt to subvert security measures in any way e.g. undertake any activities that could result or assist in the violation of any SMT policy, software licence or contract. Examples of these prohibited tools include viruses, trojan horses, worms, password breakers, network packet observers or sniffers. Examples of prohibited activities include creating ping floods; spoofing packets; performing denial-of-service attacks; forging routing information for malicious purposes; scanning for vulnerabilities; or other computer hacking techniques.

c. must not deliberately circumvent any precautions taken to prevent malicious code accessing College systems e.g. by disabling antivirus software.

d. attempt to adversely interfere with the operation of any of SMT IT services. For the purposes of this document, interfering includes wilful physical damage, wilful destruction of information, and wilful interruption of normal operations, theft and accessing restricted areas.

e. wilfully waste IT services e.g. wasting network bandwidth by downloading, printing or sending large amounts of material that is not study-related.

f. use IT services to send obscene, offensive, bogus, harassing or illegal messages.

g. use the SMT IT services for commercial purposes nor publish or circulate information about other organisations via the SMT IT services.

h. use the IT services in a way that would be considered to pose cyber threat or social engineering risk to SMT or any other party.

i. intentionally create, view, transmit, distribute, copy or store pornography or objectionable material via SMT IT services.

j. intentionally create, view, transmit, distribute, copy or store any information, data or material that violates Australian legislation (including federal legislation or Western Australian state legislation). For example, you must not view, store, send, or give access to material regarded as objectionable by the Western Australian Classification (Publications, Films and Computer Games) Enforcement Act 1996 No. 40 (e.g. sexually explicit material involving children, incitement to violence, torture, and bestiality).

k. attempt to conceal or erase the evidence of a breach of SMT IT security.

l. allow your computer or personal devices to adversely affect SMT's IT services if you are bringing your own devices to campus and utilising wireless network services provided by SMT.

m. leave personal information stored within SMT IT services after your enrolment ceases. You must make arrangements for its retention and/or removal as appropriate prior to cessation of your enrolment.

n. Use the College ICT network for the purpose of copyright infringement. If you are found to be repeatedly engaging in activities contrary to this policy, your ICT network access privileges may be suspended.

o. Connect to SMT services using a public VPN.

## 7. Compliance

To ensure student compliance with this policy, SMT reserves the right to verify compliance to this policy through various means including but not limited to monitoring student IT service activity and usage, reviewing logs, and engaging internal and/or external audit. Students acknowledge that their usage may be monitored.

Any student found to have violated this policy may be subject to disciplinary procedures as per the college By-laws and the student code of conduct.

SMT may terminate a student's IT service access and/or notify the relevant authorities if SMT staff believe that a breach has occurred.

Sanctions applied in non-IT areas may result in the removal of IT Servicers to students.

## 8. DOCUMENTS SUPPORTING THIS POLICY

### 8.1. Policies

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

### 8.2. Procedures

### 8.3. Forms

### 8.4. Other

## 9. POLICY REVIEW AND COMMUNICATION

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

## 10. POLICY APPROVAL

Approved and Endorsed:

Terry Durant

Managing Director

Date: 6/6/2023

## 11.DOCUMENT HISTORY AND VERSION CONTROL

| Version | Date Approved | Approved by | Brief Description |
|---|---|---|---|
| V1.0 | 6/6/2023 | Managing Director | Policy creation |