

Acceptable Use of Information & Technology

Written Direction No. WDICT21201

Approved by: Chief Information Officer

Approval Date: 4 June 2021

Effective From: 4 June 2021

1. Purpose

This Policy adheres to directives outlined in the [TAFE NSW Information Security Policy](#) on the TAFE NSW staff intranet.

Users of TAFE NSW information assets and digital services will fulfill their responsibilities as set out below.

2. Scope

This Policy applies to all of TAFE NSW and its [extended supply chain](#), which includes all:

- a. staff (permanent, temporary, casual and contractors);
- b. suppliers (where they manage or use our information or digital services);
- c. students;
- d. physical locations, including off-site locations where business activities are conducted;
- e. digital technologies, including communication services, networks, servers, storage, desktop and laptop computers and mobile devices; and
- f. information assets, including but not limited to digital and paper-based assets.

3. Policy

All Users will be lawful, efficient, economical and ethical in their use of TAFE NSW [information assets](#) and [digital services](#), which are provided to create, preserve, transmit and apply [knowledge](#) through administrative, teaching, research, creative works and other forms of scholarship.

The actions below are a set of user behaviours which TAFE NSW users are to follow at all times when consuming TAFE NSW's information assets and digital services.

4.1 Access and Security

Users will:

PERSONAL USE

- a. ensure that the use of TAFE NSW information assets and digital services is related to learning and/or the conduct of TAFE NSW business; and
- b. ensure that personal use of TAFE NSW information assets and digital services is kept to a minimum (e.g. operating a personal, private consulting business) and that information assets and digital services are used for genuine administration, curriculum and educational activities or the conduct of TAFE NSW business.

Users will:

SOFTWARE

- a. not modify or disable TAFE NSW information assets and digital services, and system settings provided for malware protection, software updates, or scans unless the activity is authorised by a relevant TAFE NSW ICT staff member;
- b. not make deliberate attempts to disrupt computer system performance, nor harm or destroy hardware and data in any form on TAFE NSW information assets and digital services;
- c. use only computer software or versions of software that have been authorised and tested for use on TAFE NSW information assets and digital services;
- d. never knowingly delete software on TAFE NSW information assets and digital services unless the activity is authorised by a relevant TAFE NSW ICT staff member; and
- e. never knowingly import or download unlicensed or unauthorised software on TAFE NSW information assets and digital services.

Users will:

PASSWORDS

- a. keep passwords confidential, and change them when prompted, or as required;
- b. use passwords that are not obvious or easily guessed;
- c. never allow others to use or access their personal account;
- d. shall only be provided with access to TAFE NSW information assets and digital services that they have been specifically authorised to use;
- e. log off at the end of each session to ensure that nobody else can use their account; and
- f. take reasonable precautions to lock offices, lock computers and mobile devices when not in use.
- g. shared or easily accessible passwords should be reported, and or, a failure to properly secure your password may result in disciplinary action.

Users will:

EMAIL & COMMUNICATIONS

- a. promptly inform [TAFE NSW Service Desk](#) if they suspect they have received a message that is inappropriate, or they suspect they have malware or virus infection;
- b. promptly exit an inappropriate website should a user inadvertently access such a site;
- c. never knowingly initiate or forward email or other messages containing:
 - i. a message that was sent to them in confidence, without the approval of the person who sent the message;
 - ii. computer malware, malicious attachments or links that are capable of damaging recipients' computers;
 - iii. spam, chain letters and hoax emails; and
 - iv. a message that has been altered without the knowledge of the originator.
- d. Never send or publish:

- i. unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments;
- ii. material that is threatening, bullying or harassing to another person, or makes excessive or unreasonable demands upon another person;
- iii. sexually explicit or sexually suggestive material or correspondence; and
- iv. false or defamatory information about a person or organisation.

Users will:

EDUCATION & TRAINING

- a. undertake appropriate cyber security awareness education and training annually for all TAFE NSW staff including contractors.

Users will:

CONTENT

- a. ensure that content created, transferred and used on TAFE NSW information assets and digital services is related to learning and/or the conduct of TAFE NSW business;
- b. not use unauthorised programs or intentionally download unauthorised software, graphics or music that is not associated with learning or the conduct of TAFE NSW business;
- c. ensure that services are not used for unauthorised commercial activities, political lobbying, online gaming, online gambling or any unlawful purpose;
- d. agree that some internet sites when accessing on TAFE NSW information assets and digital services may be blocked due to the nature or sensitivity of content contained or that comply with other workplace and legislation requirements;
- e. allow malware protection to scan, detect and prevent infection for all files created, transferred and used on TAFE NSW information assets and digital services;
- f. backup and store all TAFE NSW information assets to approved TAFE NSW ICT areas;
- g. allow malware protection to scan, prevent and protect electronic messaging from any malware, viruses and phishing messages. Some messages to recipients may be deleted in this process; and
- h. not create recordings of staff or students using TAFE NSW information assets and digital services without that person/s explicit permission.

4.2 Privacy and Confidentiality

Users will:

- a. never publish or disclose the email address or personal information (including names, addresses, photographs, credit card details and telephone numbers) of another person or user without that person's explicit permission;
- b. take responsibility for protecting their own personal information and not reveal personal information (including names, addresses, photographs, credit card details and telephone numbers) of themselves or others;

- c. ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests;
- d. respect the integrity of all individual emails within an email trail by not forwarding or publishing emails across the wider community; and
- e. not publish recordings of staff or students using TAFE NSW information assets and digital services without that person/s explicit permission.

4.3 Intellectual Property and Copyright

Users will:

- a. never plagiarise information (Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user without acknowledgement);
- b. respect the copyright of owners and authors of work, including works, ideas and graphics, etc., on TAFE NSW and other websites. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. Many works can only be used with the prior written permission of the author. Always acknowledge the creator or author of any material published; and
- c. not make available or use illegal (pirated) copies of copyrighted software on TAFE NSW information assets and digital services.

4.4 Ethical Behaviour

Users will:

- a. ensure that there is no conflict between what is in a user's interest and what is in the best interest of TAFE NSW and its customers;
- b. not attempt to gain unauthorised access to TAFE NSW information assets and digital services or go beyond their authorised access;
- c. not use obscene, profane, lewd, vulgar, rude, inflammatory or threatening language in public or private messages, in material published through TAFE NSW information assets and digital services;
- d. not publish information that, if acted upon, could cause damage to property or persons, nor publish deliberately false or defamatory information about a person or organisation;
- e. not engage in personal attacks including prejudicial or discriminatory attacks, not harass (distress or annoy) another person. If a user is told to stop sending messages to them, the user must stop;
- f. not use TAFE NSW information assets and digital services to access gaming or gambling sites, or material that is profane, obscene, pornographic or pedophilic, that promotes illegal acts, or that advocates violence or discrimination. Exceptions may be made where the purpose of such access is to conduct authorised research, and where written approval has been gained from an appropriate authorised person; and
- g. not use TAFE NSW information assets and digital services to send inappropriate emails including email chain letters.

4.5 Security Events

Users will:

- a. Report suspected security violations or breaches, including suspected weaknesses and vulnerabilities to the [TAFE NSW Service Desk](#).

4.6 Misuse and Breaches

Users should report any inappropriate usage or suspected misuse of TAFE NSW information assets and digital services to the [TAFE NSW Service Desk](#).

Users will be aware that:

- a. they are held responsible for their actions while using TAFE NSW information assets and digital services;
- b. they are held responsible for any breaches caused by them allowing any other person to use their account to access TAFE NSW information assets and digital services;
- c. the misuse TAFE NSW information assets and digital services may result in disciplinary or legal action which includes, but is not limited to, the withdrawal of access to services; and
- d. use of the TAFE NSW information assets and digital services to engage in any illegal act will be reported to the appropriate legal authority.

4.7 Monitoring

- a. TAFE NSW reserves the right to monitor TAFE NSW information assets and digital services for misuse under [Workplace Surveillance Act \(NSW\)](#). TAFE NSW may monitor and access individual records (such as email records, internet usage, network drives and hard drives etc.) in limited circumstances. In doing so, TAFE NSW is committed to balancing an employee’s right to privacy with the legitimate protection and proper usage of TAFE NSW resources
- b. TAFE NSW monitors individual records for the limited purposes of ensuring information security and to meet legitimate business needs.

4. Responsibilities

| Position | Responsibility |
|------------------------------------|---|
| Chief Information Officer | The Chief Information Officer is the Approver for this Policy. |
| Executive Leadership Team | The ELT is responsible for promoting a security culture |
| Chief Information Security Officer | The Chief Information Security Officer is the Contact Officer and document owner. |
| TAFE NSW Staff & System users | Staff of TAFE NSW are required to: <ul style="list-style-type: none"> • execute responsibilities as detailed in this Policy; • abide by the acceptable use of information and technology agreement, signed after induction and refreshed annually; • implement security practices as communicated within the security awareness program, including when sharing information with external parties, including government and non-government organisations; and • report suspected security violations or breaches, including suspected weaknesses and vulnerabilities. |

| Position | Responsibility |
|------------------------------|--|
| TAFE NSW Systems Group Staff | Act on reported incidents and investigate. |

5. Definitions

Definitions applying to this policy are listed and linked from in the [TAFE NSW Business Glossary](#).

6. Related documents

This policy should be read in conjunction with the following related documents:

- a. [TAFE NSW Information Security Policy](#)
- b. [NSW Cyber Security Policy](#)
- c. [TAFE NSW Social Media Policy](#)
- d. [TAFE NSW Risk Appetite Statement](#)
- e. [TAFE NSW ICT Strategic Business Plan 2020-2024](#)
- f. [Stocktake Guide](#)
- g. [Delegations Manual](#)
- h. [TAFE NSW Enterprise Risk Management Policy](#)
- i. [TAFE NSW Password Management for Users Guideline](#)
- j. [TAFE NSW Cloud Computing and Outsourcing Policy](#)
- k. [TAFE NSW Information Management Policy](#)
- l. [TAFE NSW Disaster Recovery Policy](#)

7. Contacts

Accountable Officer Chief Information Officer
 Written Direction Officer Chief Information Security Officer

8. Document information and review

This policy document will be reviewed at least every three years.

Record No. PROJ21/1244
 Review Due: 4 JUNE 2024

Approval History

| No | Effective | Approved by | Amendment |
|----|-------------|---------------------------|---------------------------------|
| 1 | 4 June 2021 | Chief Information Officer | Establishment of initial Policy |