# Information Technology Acceptable Use & Security

AIHFE seeks to provide our staff members and learners with a secure and timely access to IT equipment as well as online services and resources necessary to be able to carry out their duties and learning. AIHFE's IT facilities and services shall be used in an approved, ethical and lawful manner to avoid loss or damage to our operations, image, or financial interests and to comply with official acceptable use. Users of AIHFE's IT facilities and services shall contact the Trainer & Assessor prior to engaging in any activities not explicitly covered by these policies.

**General Information Technology Acceptable Use & Security Principles**

AIHFE strives to maintain a safe, secure and easy to use information technology systems and networking framework for our staff members and learners.

We aim to do so by ensuring:

- Adequate training is provided in the use of our IT platforms and facilities;
- Our staff members and learners have timely access to IT support; and
- Our IT systems and framework are regularly reviewed and undergo maintenance to ensure it is able to fend off any intrusions and cyberattacks, and is upgraded to recognise and incorporate the latest technologies for the benefit of our staff members and learners.

**Acceptable and Unacceptable Use of IT Facilities and Services**

- AIHFE's IT facilities and services are provided for use in the professional, administrative, commercial and community activities of the organisation. Some reasonable non-commercial personal use may be allowed, but this is a privilege and is not a right. If that privilege is abused, it will be treated as a breach of this Policy.
- The use of the IT facilities and services must not jeopardise the fair, safe and productive IT environment of our community, nor our operations, assets and reputation.
- The IT facilities and services provided must not be used unlawfully or for an unlawful purpose.
- AIHFE's IT facilities and services are provided for use in the professional, administrative, commercial and community activities of the organisation. Some reasonable non-commercial personal use may be allowed, but this is a privilege and is not a right. If that privilege is abused, it will be treated as a breach of this Policy.
- The use of the IT facilities and services must not jeopardise the fair, safe and productive IT environment of our community, nor our operations, assets and reputation.

- The IT facilities and services provided must not be used unlawfully or for an unlawful purpose.

**Security**

- AIHFE will take reasonable steps to protect the IT facilities and services from unauthorised and unacceptable use and intrusions.
- To preserve the organisation's standard operating environment and ensure compliance with licensing obligations, users of the IT facilities and services may only modify the standard configuration of any of the IT facilities and services, after first gaining approval from the IT Manager/nominated staff memeber. Users must never install or use unlicensed or malicious software on the IT facilities and must not connect unapproved networking devices to our organisation's IT infrastructure.
- Users of the IT facilities and services must not circumvent the authorised internet connection(s) or subvert our IT security measures.
- All AIHFE's IT hardware, especially portable devices, must be kept secured at all times against damage, misuse, loss or theft. In addition, hardware and software containing sensitive information or data must be protected with appropriate security measures such as passwords and encryption.

**User Responsibilities**

- It is a condition of use of the IT facilities and services that this Policy, particularly the principles of acceptable and unacceptable use, and its associated procedures must be complied with.
- Users must not:
    - Access pornographic or obscene material or material that could offend others;
    - Let anyone else use any of your accounts or tell anyone else your password;
    - Download videos, music or anything else that is copyrighted by other people;
    - Use the IT facilities to bully or harass other people;
    - Install unlicensed or malicious software;
    - Use the IT facilities to advertise for goods or services for personal purpose;
    - Forget to log out of the computer systems when you have finished using them;
    - Use the IT systems for purposes not relating to your work or learning at AIHFE; and
    - Forget to think carefully about your online conduct to protect personal information.
- Users are responsible for all activity initiating from their account.

- Users must only access the IT facilities and services using their own account.
- Users must ensure that their passwords are securely stored.
- Users of the IT facilities or services provided by a third-party provider on AIHFE's behalf must comply with any terms and conditions issued by that third-party provider.
- Users of the IT facilities and services must not create, send, store, upload, access, use, solicit, publish or link to:
    - Offensive, obscene, profane or indecent images or material;
    - Material likely to cause annoyance, inconvenience or distress to other individuals or cultures;
    - Discriminating or sexually harassing material or messages that create an intimidating or hostile work environment for others;
    - Defamatory material or material that makes misrepresentations or could otherwise be construed as misleading;
    - Material that infringes the intellectual property (including copyright) of another person or organisation;
    - Malicious software such as viruses, worms or address-harvesting software.
- The IT facilities and services must not be used in the conduct of any personal business or unauthorised commercial activities.
- The IT facilities and services must not be used for any illegal activity such as sending chain letters, breaching the SPAM Act 2003, or attacking of other computer systems.
- Staff must include the appropriate sections of the organisation's official signature and disclaimer on all e-mail messages sent.
- Electronic materials must never be forwarded on without the express or implied permission of the material's creator.
- Peer-to-peer and torrent software must only be used for lawful purposes.
- Any observed security weaknesses in or is a threat to the IT facilities and services, as well as any known or suspected breach of this Policy and its associated procedures must be reported to AIHFE as soon as practicable.

**Managing**

- AIHFE will manage user accounts, maintain a secure IT environment and keep users of the IT facilities and services informed of their user responsibilities and expected best practice standards.
- AIHFE reserves the right to investigate any and all aspects of its electronic information systems if it is suspected that any user of the IT facilities and services is acting unlawfully or violating this Policy or any other business Policy.
- AIHFE may take action it considers necessary to remedy immediate threats to the IT infrastructure or security, including suspending authorised accounts and/or disconnecting or disabling relevant IT facilities or other equipment, with or without prior notice.
- AIHFE reserves the right to block or filter any network traffic that potentially breaches this Policy or is potentially illegal.

**Consequences of Non-Compliance**

- Minor breaches of this Policy will be addressed by sending e-mails to users requesting that they desist from the breaching behaviour.
- Ongoing or serious breaches of this Policy or any other related IT Policies by any user will be addressed by the relevant disciplinary procedures.
- If a breach of this Policy, including procedures, appears to constitute an offence under State or Commonwealth law, AIHFE may (and in some cases is obliged to) refer the suspected breach to the appropriate law enforcement agency(ies).