Acceptable Use of IT Policy and Procedures

Purpose

This Policy covers acceptable use of the Central Institute of Technology and Innovation (the Institute) Information and Technology (IT) resources, the Student Management System (SMS), and the Learning Management System (LMS). This Policy represents the minimum requirements that must be met by users. Whilst the Institute does not intend to inhibit access to the Internet, IT resources, social media channels, and/or systems, the use of such services to access or attempt to access information not intended for public display or use, or to circumvent or violate the responsibilities of system users or system administrators as defined in this policy, is prohibited.

Scope

This Policy applies to all Institute users who are staff, students, and visitors, and who use any Institute IT resources, equipment, and systems.

Related Documents

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

- Academic Integrity and Misconduct Policy and Procedures
- Anti-discrimination Policy and Procedures
- Learning Management System Access and Support Policy and Procedures
- Information and Privacy Policy and Procedures
- Code of Conduct Policy and Procedures

- Student Code of Conduct Policy and Procedures

All documents referenced in this policy can be accessed via the CITI website.

Definition of Key Terms

For the purpose of this Policy, the following definitions apply:

Term	Definition
Learning Management System	A Learning Management System (LMS) is an educational software application for the development, implementation and delivery of educational courses.
Student Management System	A Student Management System (SMS) is an educational software application for the coordination of student related information including, but not limited to, grades, unit enrolments, course fees, student communication, and academic transcripts. The SMS manages student information.
System User	A system user is any Institute staff member, student, or external person who has been granted access to an Institute system for the purpose of work or study.

Policy Principles

1. **Educational and Business Purpose**
   Institute IT resources, including hardware, software, networks, the SMS, and the LMS, are provided primarily to support teaching, learning, research, and authorised administrative activities of the Institute.

2. **Lawful, Ethical, and Responsible Use**
   All use of Institute IT resources must be lawful, ethical, and consistent with the

Institute's Code of Conduct and related policies, including obligations under privacy, anti-discrimination, and academic integrity requirements.

3. **Security and System Integrity**
   Users must protect the security, integrity, and availability of Institute IT systems by following approved access controls, safeguarding credentials, and promptly reporting suspected security incidents or misuse.

4. **Respect for Privacy and Confidentiality**
   The confidentiality and privacy of personal, academic, and corporate information stored or transmitted through Institute systems must be respected at all times, in accordance with the Information and Privacy Policy and applicable legislation.

5. **Fair and Equitable Access**
   IT resources must be used in a manner that does not unreasonably interfere with or disadvantage other users, ensuring fair, reliable, and equitable access for the Institute community.

6. **Prohibition of Misuse and Unauthorised Activity**
   The unauthorised access, modification, disruption, or misuse of IT systems, data, or networks is strictly prohibited, including attempts to bypass security controls or access information not intended for the user.

7. **Accountability and Compliance**
   Users are accountable for all activity undertaken using their Institute credentials or access permissions and must comply with this Policy, associated procedures, and any lawful directions issued by the Institute.

8. **Monitoring and Enforcement**
   The Institute reserves the right to monitor, audit, and restrict use of IT resources to ensure compliance with this Policy, manage risk, and protect institutional systems, subject to applicable privacy and legal obligations.

Policy Statement

IT resources, social media channels, SMS and LMS, and computer resources together with access to the Internet at the Institute are primarily for educational purposes. Information about the access to and acceptable use of IT resources, SMS, and LMS will be incorporated into staff and student training, printed materials, and related online resources.

1. System User Responsibilities

Institute system users are responsible for being aware of, and complying with:

1.1 Ensuring that their usage complies with this Policy and Procedures, and for informing the Institute when they cease their association with the Institute.

1.2 Reporting any suspected security problems or unacceptable use to the Institute's IT Support, and not demonstrating the problem to others.

1.3 Respecting the physical hardware and network configuration of Institute owned network.

1.4 Not extending the physical network on which their system resides.

1.5 Not performing any unauthorised, deliberate action that damages or disrupts a computer system, alters its normal performance, or causes it to malfunction.

1.6 Not using systems to gain unauthorised access to other computers, networks or information regardless of the intention.

1.7 Not infringing copyright.

1.8 Not using any of the Institute's official branding materials on their personal webpages, email, or other messaging facilities.

1.9 Being aware that electronic mail in its present form is not secure and is vulnerable to unauthorised access and modification.

1.10 Any user who believes their files have been tampered with should immediately change their password and contact IT Support with the specific details.

2. System User Accounts

Users are ultimately accountable for all actions attributed to their User Account. To support this, users are responsible for safeguarding their passwords and/or other sensitive access control information related to their accounts or network access. As such, system users must recognise the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share, or divulge such information. Any attempt to conduct such actions by a system user is a breach of this Policy and Procedures and may result in misconduct. Users shall ensure access privileges are restricted to their own use only. The following principles apply:

2.1 System users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorised computer and network access privileges to others.

2.2 System users must not implant, execute, or use software that allows them unauthorised remote control of Institute computer and network resources, or of accounts belonging to others.

2.3 System users must not implant, execute, or use software that captures passwords or other information while the data are being entered at the keyboard or other data entry device.

2.4 System users must not obtain nor attempt to obtain any electronic communication or information not intended for them.

2.5 System users must not attempt to intercept or inspect information enroute through computer and network resources, nor use the Institute's computer and network resources to attempt to intercept or inspect information enroute through networks elsewhere.

2.6 If specific access is required, the appropriate staff member should be contacted rather than disclosing a password.

2.7 Unattended workstations must always be logged off or left in the Workstation Locked mode when the operator leaves their workstation unattended.

2.8 Users must be aware that removable storage like USB connected media, flash drives, CDs or DVDs are a security risk, and users are responsible for them.

2.9 Where staff have confidential data stored on the removable storage, then the staff member may be required to encrypt the data. Sensitive information stored on portable devices (e.g., laptops, PDAs) should be encrypted.

2.10 Any user who believes that their files have been tampered with, should change their password as soon as practicable and contact IT Support with the specific details.

3. System User Passwords

All passwords must meet the following minimum standards:

3.1 All accounts (e.g., computers and LMS) must have passwords.

3.2 Passwords for accounts must not be shared, unless a team account has been specifically authorised in writing.

3.3 System users are encouraged to regularly change the passwords for user accounts.

3.4 Passwords should, where possible, use a mix of alpha and numeric characters and contain at least 6 characters if the operating system supports passwords of that length.

4. IT Systems Permissions

System Users will only have access to the information and systems that they need to perform their function. Elevated local access permissions (e.g., administration for the SMS and the LMS) will only be granted for essential and specific purposes. The following principles apply:

4.1 System users may not copy any information or software stored on their desktop or laptop computer, for personal use.

4.2 System users may not use the Institute's systems for any of the following activities:

4.2.1 Gambling or any form of Internet gaming.

4.2.2 Share trading.

4.2.3 Copyright infringement.

4.2.4 Use any of the Institute's systems for personal financial gain, solicitation, or private business purposes.

5. Inappropriate Material

5.1 System Users must not access, create, download, print, store, forward or send inappropriate content. Examples of which include, but are not limited to:

5.1.1 Information or images containing indecent material (this includes pornographic or other sexually explicit material), or other material, which explicitly or implicitly refers to sexual conduct or preference.

5.1.2 Information or images containing profane of abusive language. This includes anything that refers to or supports discrimination of any kind.

5.1.3 Unwelcome propositions to staff, students, and members of the broader community.

5.1.4 Any defamatory, illegal, offensive, annoying, or harassing material.

5.1.5 Information intended to incite criminal activities or instructs others how to commit such acts.

5.1.6 If a system user is in doubt as to whether the material that they are accessing is inappropriate, it should be treated as such and remove it from the computer.

5.1.7 Staff who receive inappropriate material must advise their supervisor that they have received or accessed such content.

5.1.8 Students who receive inappropriate material must advise their Unit Coordinator and/or Student Services that they have received or accessed such content.

6. The Learning Management System (LMS)

The LMS is part of the Institute's intellectual property and an integral part of the student learning experience. As such, staff and students must ensure that they use the LMS for educational purposes only; as per the level of permission granted; and as directed. It is an expectation that students will:

6.1 Engage with learning content on the LMS as directed by the Institute.

6.2 Notify staff of any problems with accessing and engaging with material.

6.3 Make a serious attempt to submit assessments as per the unit instructions and retain a copy (i.e., screenshot or similar) of assessment submission.

6.4 Refrain from making inappropriate posts on discussion boards that deliberately attempt to subvert the discussion thread.

6.5 Refrain from redistributing assessments.

6.6 Not abuse, insult, threaten, participate in ongoing teasing, or criticise peers and/or staff, either verbally or in written form

6.7 Adhere to the Institute's guidelines on academic integrity and referencing.

6.8 Refrain from deleting or removing content or discussions without the express permission of the lecturer, unless it is to edit and re-submit work.

6.9 Not download and redistribute learning materials to peers or outside sources for your own private gain or that of another student or outside source.

7. Email, discussion board posts, social media, and online communication

Emails, social media posts, and discussion board posts must be written with the same consideration as any physical communication. System Users, both staff and students, should ensure that all online communication is free from harassment and discrimination in any form. Staff and students should be aware that sending or posting threatening, rude, or inappropriate content to and/or about staff and peers may result in misconduct. When interacting on social media whether it is on an Institution social media channel or on a private site, staff and students must refrain from:

7.1 Posting inappropriate material.

7.2 Posting images of individual staff and/or students without their prior consent.

7.3 Posting photos or comments that may cause harm to an individual or group of individuals (unflattering photos or comments).

7.4 Posting comments or photos that may be defamatory to the Institution, staff, and or students.

8. Legal Requirements

8.1 For legal purposes, emails, discussion board posts, and other written communication have the same standing in court as paper documents. Users must be aware that the Institute can be involved in litigation.

8.2 Any records relating to use and activities in relation to email, internet and intranet are discoverable by way of court order or subpoena. These include matters affecting legal proceedings, affecting personal affairs of employees, parents, students, or third parties, as well as relating to research, or other communications even if communicated in confidence.

8.3 Emails and discussion board posts residing on or transmitted across the Institute's system are the property of the Institute.

9. Information and Privacy

System Users must adhere to the Institute's policies and procedures relating to information and privacy.

Procedures

Nil

Related Legislation

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

- Higher Education Standards Framework (Threshold Standards) 2021
- Education Services for Overseas Students Act 2000

- Copyright Act 1968
- Anti-Discrimination Act 1977
- Privacy and Personal Information Protection Act 1988
- Criminal Code Act 1995

Change and Version Control

Version	Date Approved	Authored by	Approved by	Description
1.0	14/03/2023	Chief Executive Officer	Board of Directors	Corporate Policy

Policy Information

Author	Chief Executive Officer
Responsible Officer	Chief Executive Officer
Approved by	Board of Directors
Approval date	14/03/2023
Status	Approved (Current Version)
Next review due	13/03/2026

Name of Policy	Acceptable Use of IT Policy and Procedures	
Version	V1.0	
Policy: **Corporate**	Date: 14/03/2023	Status: Final ratified by the Board of Directors on 14/03/2023

File: Acceptable Use of IT Policy and Procedures_V1.0