WENTWORTH INSTITUTE
OF HIGHER EDUCATION

WIN EDUCATION CRICOS CODE 03279M PRV12063

Document: Acceptable Use of ICT Policy		
Approved by:	**Version:1.0**	**Date: 09.2023**

Purpose

The purpose of this document is to set appropriate acceptable use parameters for the Information Technology systems, to ensure the continued effective and secure operation of those systems and to protect the WIN Institute of Higher Education from problems such as error, fraud, defamation, breach of copyright, unlawful discrimination, illegal activity, privacy violations and service interruptions.

Scope

These guidelines apply to:

- all users
- any use of the systems, whether or not during business hours, on WIN Institute of Higher Education premises or through the use of privately owned devices or facilities.

Authorised use

The systems are primarily a WIN Institute of Higher Education tool, to be used for WIN Institute of Higher Education purposes by students, staff and affiliates.

- In the case of staff, this includes uses relevant to their employment with the WIN Institute of Higher Education
- In the case of students, this includes uses relevant to their enrolment and course activities.
- In the case of affiliates, this includes uses for the purpose for which they have been given access to the systems.

Personal use

Any personal use of WIN Institute of Higher Education equipment and systems should be incidental and not interfere with the users role within the WIN Institute of Higher Education, the work or study of others or the operation of the systems.

However, unreasonable or excessive personal use is not permitted. For example, the systems must not be used to conduct a personal business or private commercial activity, gamble, objectionable material or carry out excessive and regular research into topics not related to work or study.

Ownership of data and intellectual property

Subject to the WIN Institute of Higher Education's statutes and regulations, the WIN Institute of Higher Education is the owner of all data:

- created by employees as part of their employment; and
- the intellectual property created by staff or students created as part of their employment of academic activities.
- created, sent or received by users using the systems,

and all such data may be accessed as records of evidence, including in an investigation or in response to other actions such as audit, litigation or criminal investigations.

Conditions of access

It is a condition of access to the systems that users must agree to comply with all WIN Institute of Higher Education policies relating to the use of computing facilities, including the Student Handbook and these guidelines.

Users:

- are presumed to be responsible for all activities undertaken using their accounts
- must take reasonable steps to keep their account secure
- must choose a password that cannot easily be guessed or predicted
- must not share their password with anyone else or record their password in obvious locations
- must change their password regularly (and immediately if it becomes known by another person)
- must not permit other persons to use their account (other than through an email proxy arrangement or unless approved in advance by the Dean or CEO.
- must log out or lock their computers whenever they are left unattended
- must protect the security of data held on mobile systems (eg phones, laptops, memory sticks and other storage mediums), including by maintaining reasonable virus control measures where possible
- must not copy or export any official electronic communication or Wentworth data for non-official purposes and the same must not be retained once the official purpose is fulfilled
- Wentworth data must not be copied to unauthorised devices
- must not connect unauthorised devices to the network, either via software or hardware that makes this possible (eg attaching a personal computer or external storage device)
- must make sure that important WIN Institute of Higher Education data that is not included in automatic backups is manually backed up on a regular basis and can be recovered to the latest version in the event of data loss
- must not use abusive, profane, threatening, racist, sexist, or otherwise objectionable language in any message
- must not access, send, receive, store, or print pornographic, racist, sexist, or otherwise discriminatory, or objectionable material
- must report actual or suspected security breaches to the IT Service Desk as soon as possible
- must not defeat or attempt to defeat security restrictions on systems and applications
- must not remove or disable antivirus and other similar client security agents without approval from the CIO
- must not use or install unauthorized or unlicensed software

- knowingly propagate or disseminate malicious software of any type

Unauthorised and illegal uses

Users must not use the systems to engage in offensive, unlawful or illegal behaviour.

Email and other electronic communications

Email is an official method of communication for staff and students. Bulk emails to students must be authorised by the Dean or Registrar before sending to students.

Privacy

Users must deal with personal information in accordance with the NSW Privacy Act 2018.

Access, monitoring, filtering and blocking

Users:

- use the systems on the understanding and condition that their use is monitored
- acknowledge and consent to the WIN Institute of Higher Education's right to access, monitor, filter and block electronic communications created, sent or received by any user using the systems
- acknowledge that student access is provisioned when commencing at the WIN Institute of Higher Education, and student access will be removed after graduation or withdrawal from a course
- acknowledge that staff and contractor access is provisioned when commencing at the WIN Institute of Higher Education, and staff and contractor access will be removed on their last day of employment
- acknowledge that remote access to the WIN Institute of Higher Education's network may only be made by IT approved VPN clients/services.

Subject to the approval and at the discretion of the Dean or other authorised person and for compliance with applicable legislation, the WIN Institute of Higher Education reserves the right to (without notice):

- intercept, access, monitor and use electronic communications created, sent or received by users of the systems in any manner determined by the WIN Institute of Higher Education (including as records of evidence in an investigation or in response to other actions such as audit, litigation, criminal investigations or freedom of information requests)
- monitor the use of any device or terminal
- inspect any data residing on any WIN Institute of Higher Education-owned resource (regardless of data ownership and including personal emails and other personal communications and data stored in personal file directories)
- capture and inspect any data in any computing infrastructure owned by the WIN Institute of Higher Education
- delete or modify any data in its network
- re-image its desktops and laptops as and when required
- apply filtering systems to the network that limit use and activity by preventing communications based on size or content.

For example, communications may be blocked if they are suspected:

- to contain unlawful material
- to be unsolicited commercial electronic messages within the meaning of the Spam Act 2003.
- establish processes to block access to websites deemed inappropriate.

For example, the WIN Institute of Higher Education may block access to:

- websites deemed to be a security risk
- websites that may cause a negative impact on the systems
- websites that affect network bandwidth detrimentally
- websites deemed to contain offensive or unlawful material
- internet protocols and methods deemed insecure
- websites that contravene the WIN Institute of Higher Education's policies in any way
- remove any material deemed to be offensive, indecent or inappropriate (including obscene material, defamatory, fraudulent or deceptive statements, threatening, intimidating or harassing statements, or material that violates the privacy rights or property of others)
- check, filter, block and moderate comments and conversations published through WIN Institute of Higher Education controlled channels and media and remove content that is in breach of applicable laws, codes and policies.

The WIN Institute of Higher Education also collects utilisation statistics based upon network address, network protocol application use or user-based.

Destruction of WIN Institute of Higher Education data

Users who store WIN Institute of Higher Education data on a privately owned device or facility are responsible for ensuring that the WIN Institute of Higher Education data is rendered illegible and irretrievable at the time of disposal of that device or facility.

Destruction of Damage of WIN Institute of Higher Education IT Property or Assets

Users who deliberately or accidently damage or break WIN IT Equipment including but not limited to Phones, Laptops, Computers, Networks, security cameras, telephone systems are liable for damage caused, and may be requested to pay a reasonable sum towards replacement costs or repairs.

Breach of these guidelines

Access to the systems may be suspended or terminated at any time if these guidelines are breached. In addition:

- staff who breach these guidelines will be referred to the Dean and/or CEO and dealt with in accordance with processes in relation to misconduct or unsatisfactory performance (whichever is applicable).
- affiliates who breach these guidelines will be referred to the Dean and/or CEO dealt with in accordance with the relevant processes
- students who breach these guidelines may be subject to sanctions under the Student Non-Academic Misconduct Policy.

A breach of these guidelines may also be:

- a breach of third party rights (such as an infringement of intellectual property rights)
- a criminal offence (such as serious acts of harassment, bullying and occupational violence and vilification).

In addition to any disciplinary action by the WIN Institute of Higher Education, this may lead to civil or criminal proceedings and penalties, which the WIN Institute of Higher Education may report to relevant law enforcement bodies and for which the user will be held personally accountable.

In some exceptional circumstances (for example where access to objectionable material relates directly to a user's employment or study with the WIN Institute of Higher Education), subject to the approval of and at the discretion of authorised persons, an exemption may be granted for activities that would otherwise breach these guidelines. Exemptions may be required to be approved in advance by the Dean.

Complaints

Users who receive an internal or external electronic communication that is offensive or inappropriate, should in the case of staff and affiliates, raise it with the Dean, or in the case of students, with the Registrar.

Publication

The Academic Integrity and Student Misconduct policy and procedure will be published on WIN Higher Education website at www.win.edu.au.

Legal and Policy Framework

- Australian Qualifications Framework (AQF)
- Higher Education Standards Framework (Threshold Standards) 2021
- Tertiary Education Quality and Standards Agency Act 2011
- TEQSA Acts and Standards
- Education Services for Overseas Students Act 2000 (ESOS Act)
- The National Code of Practice for Registration Authorities and Providers of Education and Training to Overseas Students 2018 (National Code 2018)

Related Documents

- Academic Integrity and Student Misconduct Policy
- Student Non-Academic Misconduct Policy
- Academic Grievance Handling Policy and Procedure for Students
- Whistleblower Policy and Procedure