Policy Title: **Acceptable Use of Information Systems**

Policy Owner: **Chief Information Officer**

Keywords: **Access, Authorised, Communication, Information Systems, Private Usage**

Policy Code: **PL268**

Intent
Organisational Scope
Definitions
Policy Content
Accountabilities and Responsibilities
Related Documents
Contact Information
Approval History

1. INTENT:

Edith Cowan University (ECU or the University) provides access to Information Systems primarily for University-related teaching, research, academic, professional and business purposes. This policy does not seek to inhibit or unnecessarily restrict use of Information Systems. The intent is to inform the University Community about minimum levels of acceptable behaviour and protections around the use of University Information Systems.

2. ORGANISATIONAL SCOPE:

This policy and its associated operational documents apply to all Authorised Users of the University's Information and Communication Technology (ICT) environment.

Included in scope are all University Information Systems, regardless of their location, and any devices connected to the University's networks, including where members of the University Community bring their own devices for use whilst at the University.

3. DEFINITIONS:

The University Glossary and the following definitions apply to this policy.

Term:	Definition:
Authorised Users	Any person who has been granted access to University information assets or any part of the University's ICT environment by a person authorised by the University to grant that access.

Digital Communication Channels	Tools that allow for communication using electronic transmission of information such as email and social media.
Information Assets	Information which has been collected within a system or other digital repository, and that has a value to the University.
Information and Communications Technology (ICT)	Any device, network, system, service, infrastructure, application, database or any physical and/or virtual location that stores, transports or processes University Information Assets.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction, in order to provide confidentiality, integrity and availability.
Information Systems	An Information System is any organised system for the collection, organisation, storage, and communication of information. An Information System may or may not be provided by the University but is provided to Authorised Users to assist in the delivery of University business.
Private Usage	Usage that is of a personal nature and not primarily for University-related teaching, research, academic, professional, or business purposes.

4. POLICY CONTENT:

General:

4.1. The University monitors its ICT environment, including usage of the environment, as a component of ensuring adequate Information Security and effective management of Information Assets. All reasonable steps are taken to protect the privacy and confidentiality of Authorised Users.

4.2. Authorised Users of the University's ICT environment are expected to:

a. take reasonable steps to ensure they understand this policy, and are abiding by its intent when making decisions and/or taking actions;
b. seek advice prior to acting if there is any doubt about whether a proposed use is permitted or authorised;
c. advise the Chief Information Officer (CIO) or their nominee of any activities and practices that are reasonably believed to contravene this policy.

4.3. Authorised Users must use the University's ICT environment in a manner which:

a. is lawful;
b. aligns with the University's values and reflects positively on the University's reputation;

c. does not intentionally create an intimidating or hostile work or study environment for others; and
d. supports the provision of a fair, safe and productive environment within which all staff and students can work or study.

4.4. Authorised Users must not use the University's ICT environment in a manner which could reasonably be suspected to be inappropriate including:

a. accessing pornography;
b. intentionally downloading, storing, distributing or viewing material that can reasonably be perceived to be offensive, obscene, indecent or menacing such as material that incorporates gratuitous violence, material that is discriminatory and material involving racial or religious vilification;
c. stalking, blackmailing or engaging in any form of threatening behaviour;
d. transmitting spam or other unsolicited communications;
e. introducing or distributing security threats, including a virus of other harmful malware; or
f. without authority accessing, copying, altering or destroying University Information Assets.

4.5. The University provides access to Information Systems primarily for University-related teaching, research, academic, professional, or business purposes. While a reasonable level of Private Usage is permitted, Private Usage is a privilege and must:

a. be kept to a minimum and not interfere with productive use of resources or the delivery of expected University outcomes;
b. not result in an unnecessary or avoidable financial cost to the University; and
c. comply with clause 4.4 (above).

4.6. As far as reasonable and practicable, and in accordance with the Information Security and Information Technology policy, University sanctioned, and protected Information Systems must be used for the storage of University-related data and information.

Access to Information Systems:

4.7. The University reserves the right to decide who will and will not be provided access to University Information Systems and to remove access should the University deem access to no longer be required or to no longer be in the University's best interests.

4.8. Authorised Users provided with accounts enabling access to University Information Systems accept accounts on the understanding they are for the exclusive use of the Authorised User and must not be shared or used by anyone other than the Authorised User.

4.9. Passwords, accounts and documented processes required for the access of University information must be protected and secured in accordance with the conditions under which access has been provided.

4.10. Authorised Users must not deliberately avoid or attempt to avoid authentication or conceal or attempt to conceal their identity whilst using University information Systems.

4.11. Authorised Users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise Information Security.

4.12. Authorised Users who reasonably suspect the privacy and security of their account has been compromised must immediately report their concern to the CIO or their nominee.

4.13. A University identity card must always be carried when using on-campus computing facilities. Authorised Users unable to show a current and valid University identity card to security officers and/or other University staff on request may be required to leave the facility immediately.

4.14. Persons seeking entry to a computing facility where use of an access card is required to gain entry must use their own access card. Accessing a facility using a card other than the Authorised User's own access card is considered unauthorised access.

4.15. Authorised Users who access the University's ICT environment remotely must avoid accessing or creating sensitive University Information Assets from shared devices or publicly accessible systems.

4.16. Authorised Users who access/store University information using a personal device must do so in accordance with the Information Security and Information Technology policy.

Digital Communication Channels:

4.17. Members of the University Community communicating from a University provided account must ensure the way they communicate reflects positively on the University and upholds the University's values.

4.18. All communications are regarded as University records. Users of the University's ICT environment accept that there are legislative requirements which may oblige the University to disclose information contained in any such communications.

4.19. Users of the University's ICT environment must take all reasonable steps to ensure information reasonably believed to be confidential, sensitive, or to present a risk to the University should it be accessed by entities other than the intended recipient, is only conveyed using Information Systems that are protected and secure.

4.20. Staff must be aware agreements made in digital communications channels, for example, email, can be considered legally binding on the University and must only make offers and agree to undertake actions reflective of the level of authority and decision-making powers vested in them by the University.

4.21. Staff must seek approval from the relevant senior executive prior to sending a global staff email.

Breaches and exceptions:

4.22. Non-compliance with this policy by an Authorised User will be investigated and, subject to the applicable provisions of relevant legislation, statutes, rules, policies and industrial agreements, action may be taken, up to and including termination of a staff member's employment and cancellation of a student's enrolment.

4.23. Excessive Private Usage of Information Systems, which, by its nature, is not reasonably justifiable as being for University required or related educational, research, professional or business purposes, may be investigated and treated as an act of non-compliance with this policy.

4.24. Authorised Users with a legitimate need to access a restricted or filtered site must request permission from the CIO, or their nominee, to have their access authorised. The University reserves the right to determine if access will be authorised.

5. ACCOUNTABILITIES AND RESPONSIBILITIES:

The CIO is the policy owner and has overall responsibility for taking all reasonable steps to ensure this policy and its associated operational documents are achievable, understood, and accessible by the persons falling within the scope of the policy.

Users of University information Systems are responsible for taking all reasonable steps to understand this policy and related documents, and proactively seek guidance should there be uncertainty around any aspect of application.

6. RELATED DOCUMENTS:

The following documents should be read and understood in conjunction with this policy:

Staff Code of Conduct
Copyright – Online High-Use Collection policy
Fraud and Misconduct Prevention and Management policy
Information Security and Information Technology policy
Management of Misconduct and/or Serious Misconduct (staff)
Privacy policy
Relevant Industrial Instruments
Social Media policy
Statement on Academic Freedom and Freedom of Speech
Student Code of Conduct
University Statute No. 22 - Student Conduct

7. CONTACT INFORMATION:

For queries relating to this document please contact:

Policy Owner	Chief Information Officer
All Enquiries contact:	Vito Forte
Telephone:	6304 3737
Email address:	v.forte@ecu.edu.au

8. APPROVAL HISTORY:

Policy approved by:	Vice Chancellor
Date policy first approved:	December 2000
Date last modified:	29 March 2021
Revision history:	• June 2008 • July 2016 • December 2018 – Addition of clarification of storage • March 2021 Comprehensive review and refresh of the policy including removal of operational information and re-drafting as a principle-based policy.
Next revision due:	April 2024
HPCM file reference:	SUB/73511