Policy Title: Acceptable Use of Information Systems

Policy Owner: Chief Information Officer

Keywords: Acceptable Use, Authorised, Information Systems, Personal Conduct

Policy Code: PL268 / it049

1. INTENT

This policy guides and directs acceptable use of University Information Systems.

2. ORGANISATIONAL SCOPE

This policy is applicable to all Users of University owned and managed Information Systems including, but not limited to, University Students, Staff, Council Members and Contractors.

3. DEFINITIONS

TERM	DEFINITION
Copyright	The exclusive legal right, given to an originator or an assignee to print, publish, perform, film, or record literary, artistic, or musical material, and to authorise others to do the same
ECU	Edith Cowan University 'the University'
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 for the purpose of Users to conduct ECU business
User	Any person that accesses the services provided by the ECU Information Systems

4. POLICY CONTENT

This policy applies to all Information Systems owned and/or managed by the University, regardless of their location and any devices connected to the University's networks.

4.1 Personal Conduct

4.1.1 Any use of ECU Information Systems must be in accordance with University policy including but not limited to the ECU Code of Conduct, Email Policy, Copyright Policy, Social Media Policy, Privacy Policy and the Information Security Policy;

4.1.2 When accessing the Internet from ECU Information Systems, Users must act in accordance with relevant University standards, values and rules as required by their role; and

4.1.3 When using information services that are supplied on a shared basis - for example shared laboratory computers, Users must comply with all written rules and guidelines for the facility.

4.2 Access to Information Systems

4.2.1 User accounts enabling access to the University's Information Systems are for the exclusive use of an authorised User and must not be shared or used by others;

4.2.2 Users must take reasonable precautions to ensure that passwords, accounts and data are adequately secured;

4.2.3 Users must not deliberately attempt to avoid authentication or to conceal their identity whilst using any University Information System;

4.2.4 Users with access to privileged and/or proprietary information on University Information Systems must make all reasonable attempts to maintain the security and confidentiality of that information;

4.2.5 Any attempt to gain unauthorised access to University Information Systems, or attempts to purposefully discover and exploit any security vulnerabilities in University Information Systems will be treated by the University in accord with the Fraud and Misconduct Prevention and Management Policy (staff) and Statute 22, Student Conduct (academic).

4.2.6 A University identity card must be carried at all times when using on-campus computing facilities. Users unable to produce a valid identity to security officers and/or other University staff will be required to leave the facility;

4.2.7 Any person using computing facilities that require an access card for entry must use his/her own card to gain entry;

4.2.8 Users of University remote access services must avoid accessing or creating sensitive University information from shared devices or publically-accessible systems; and

4.2.9 For the purposes of enforcing this policy and to meet the University's legal and regulatory requirements, the University reserves the right to monitor Information Systems and technology usage and to examine any information gathered from that monitoring;

4.3 Breaches

4.3.1 Failure to adhere to the policy conditions, inadvertently or otherwise, may be considered an act of misconduct and action may be taken in accordance with relevant laws and University statutes, by-laws, rules, policies and procedures; and

4.3.2 Where required by law, the University may report or disclose breaches of this policy to third parties such as law enforcement agencies, the Privacy Commissioner, Public Sector Commission and the Corruption and Crime Commission.

5. ACCOUNTABILITIES AND RESPONSIBILITIES

The Policy Owner has overall responsibility for the content of this policy and its operation in the University.

All Users are required to comply with the content of this policy and to seek guidance in the event of uncertainty as to its application.

6. RELATED DOCUMENTS:

6.1 The policy is supported by the following documents:

Users of University systems to which this Acceptable Use of Information Systems Policy applies are strongly encouraged to read and make themselves familiar with the following related policies:

- Information Security Policy
- Email Policy
- Code of Conduct
- Social Media Policy
- Misconduct and Serious Misconduct – General Staff HR153
- Fraud and Misconduct Prevention and Management Policy
- Privacy Policy
- Academic and Professional Staff Union Collective Agreement 2013

7. CONTACT INFORMATION

For queries relating to this document please contact:

Policy Owner	Chief Information Officer
All Enquiries Contact:	Manager, Information Security
Telephone:	08 6304 3590
Email address:	k.stones@ecu.edu.au

8. APPROVAL HISTORY

Policy Approved by:	Vice Chancellor
Date Policy First Approved:	December 2000
Date last modified:	July 2016
Revision History:	June 2008 July 2016
Next Revision Due:	July 2018
TRIM File Reference	SUB/73511