Southern Cross Education Institute
Higher Education

530-538 Victoria Street, North Melbourne, VIC, 3051, Australia.
155-161 Boundary Road, North Melbourne, VIC, 3051, Australia.
41 Boundary Road, North Melbourne, VIC, 3051, Australia.
14-16 Grote Street, Adelaide, SA, 5000, Australia.

Email: info@scei-he.edu.au
Web: www.scei-he.edu.au
Phone: +61 3 9602 4110 (Melbourne) / +61 8 8212 8745 (Adelaide)

ICT Use Policy and Procedure HEPP44

PURPOSE

This policy establishes Southern Cross Education Institute (Higher Education) (SCEI-HE)'s principles for the responsible and ethical use of ICT resources. It ensures ICT supports teaching, learning, research, and administrative activities while maintaining security, privacy, accessibility, and compliance with legal and regulatory requirements, including the **HESF 2021 Standards**. The policy also outlines responsibilities, expected behaviours, and consequences for misuse.

SCOPE

This policy applies to all staff, students, and contractors of SCEI-HE who access ICT resources, facilities, or services on SCEI-HE premises or remotely.

DEFINITIONS

SCEI-HE	Southern Cross Education Institute (Higher Education)
Acceptable use	Use of ICT resources is consistent with SCEI-HE's teaching, learning, research, consultancy, and administrative objectives, including incidental personal use that does not interfere with institutional operations.
Acceptable use	Any person accessing SCEI-HE ICT resources, including staff, students, consultants, contractors, and other authorised users.
User	Any person accessing SCEI-HE ICT resources, including staff, students, consultants, contractors, and other authorised users.
ICT resources	Information and communication technology assets provided by SCEI-HE, including physical and digital spaces, software, devices, networks, and storage systems.
ICT facilities and services	ICT facilities, equipment, and services owned or leased by SCEI-HE, and user-owned devices connecting to SCEI-HE networks.
Collaboration services	Communication tools enabling information exchange, including videoconferencing, messaging, voicemail, and screen sharing.

POLICY

General Principles

SCEI-HE ICT resources are critical for achieving institutional objectives. Users must:

1. Comply with Australian laws, including copyright, privacy, and cybersecurity legislation.
2. Use ICT resources ethically, responsibly, and in alignment with SCEI-HE's mission and values.
3. Protect the confidentiality, integrity, and availability of SCEI-HE data and systems.
4. Recognise that ICT use is monitored and that misuse may result in disciplinary or legal action.
5. Ensure accessibility and inclusive use of ICT tools in accordance with HESF Standard 4 requirements.
6. Support continuous improvement by reporting risks, vulnerabilities, and incidents promptly.

ICT Use Code of Conduct

Expectations:

Users must:

- Adhere to relevant legislation and SCEI-HE policies.
- Report viruses, security incidents, or ICT malfunctions to IT Services.
- Use ICT resources only for authorised purposes.
- Ensure reasonable use of shared ICT resources.
- Take precautions to protect sensitive information from unauthorised access.
- Accept responsibility for all activity originating from their accounts.

Prohibited behaviours:

Users must not:

- Attempt unauthorised access to SCEI-HE or external systems.
- Download or transmit copyrighted or illegal materials.

530-538 Victoria Street, North Melbourne, VIC, 3051, Australia.
155-161 Boundary Road, North Melbourne, VIC, 3051, Australia.
41 Boundary Road, North Melbourne, VIC, 3051, Australia.
14-16 Grote Street, Adelaide, SA, 5000, Australia.

Email: info@scei-he.edu.au
Web: www.scei-he.edu.au
Phone: +61 3 9602 4110 (Melbourne) / +61 8 8212 8745 (Adelaide)

- Share passwords or misuse loaned ICT equipment.
- Engage in harassment, discrimination, or offensive communications via ICT.
- Introduce malware, spam, or malicious software.
- Use ICT resources for unauthorised commercial activities.

Acceptable use of specific services:

Internet:

- Provided for academic, research, and administrative purposes.
- Access is monitored; users must not access pornography, racially insensitive, or offensive material unless authorised for teaching/research purposes.

Email:

- SCEI-HE email accounts are for official purposes only.
- Personal use is prohibited.
- Offensive, discriminatory, or harassing emails are prohibited.
- Users must avoid opening suspicious attachments or links.

Phone services:

- Provided for business purposes only.
- Harassing or malicious calls are prohibited.
- International calls require prior approval.

Collaboration services:

- Messaging, video conferencing, and screen sharing are for authorised academic or administrative use.
- Sensitive or commercial information must not be shared through these tools unless authorised.
- All collaboration activities are monitored and archived according to record management requirements.

Compliance and Breaches

- Breaches may result in disciplinary action under:
  - HEPP07 Student Conduct Policy
  - HEPP10 Workplace Investigations Policy and Procedure
  - HEPP47 Student Misconduct Policy and Procedure

PROCEDURE

Procedures

Reporting breaches

- Users report breaches to the IT Manager or direct line manager.
- IT Manager investigates, documents, and reports incidents to relevant governance committees if necessary.

Incident management

- Breaches are classified by severity:
  - Minor breaches: warnings, counselling, and training.
  - Major breaches: formal disciplinary action per relevant policies.
- High-risk incidents escalate to senior management or regulatory authorities as required.

Monitoring and auditing

- All ICT activity is logged and may be monitored.
- IT Manager conducts periodic audits to ensure compliance with this policy and HESF obligations.

Training and awareness

- Users receive induction on ICT policy, cybersecurity, and data privacy.
- Regular updates and reminders are provided via email, staff portal, or workshops.
- Training addresses accessibility, inclusivity, and safe ICT practices.

Continuous improvement

- ICT risks, incidents, and policy compliance outcomes are reviewed annually by IT Services and reported to the Academic Board and Corporate Board in line with HESF governance requirements.

RELATED DOCUMENTS

Student Conduct Policy HEPP07

Workplace Investigations Policy and Procedure HEPP10

Student Misconduct Policy and Procedure HEPP47

530-538 Victoria Street, North Melbourne, VIC, 3051, Australia.
155-161 Boundary Road, North Melbourne, VIC, 3051, Australia.
41 Boundary Road, North Melbourne, VIC, 3051, Australia.
14-16 Grote Street, Adelaide, SA, 5000, Australia.

Email: info@scei-he.edu.au
Web: www.scei-he.edu.au
Phone: +61 3 9602 4110 (Melbourne) / +61 8 8212 8745 (Adelaide)

LEGISLATIVE CONTEXT
Copyright Act 1968 (Cth) Privacy Act 1988 (Cth) Other relevant Australian ICT and cybersecurity legislation

RESPONSIBILITIES
Managers: • Responsible for reporting any security incidents or breaches of this policy by staff under their supervision to the IT Manager. IT Manager: • Responsible for monitoring user compliance with this policy and investigating and reporting breaches of this policy. Users: • Responsible for reporting any security incidents and breaches of this policy to the IT Manager or their direct line manager.

DOCUMENT AND RECORD CONTROL	
Created	March 2016 (V1.0)
Amended	February 2016 (V1.1); February 2021 (V2.0), Sep 2025 (V2.1)
Last reviewed by	Quality Assurance and Compliance Unit (Sep. 2025)
Last approved by	Academic Board (Sep. 2025)
Version	2.1
Effective date	Sep. 2025
Next planned review	Sep. 2027