SCEI
SOUTHERN CROSS
EDUCATION INSTITUTE

Melbourne: 155-161 Boundary Road, North Melbourne VIC 3051
41 Boundary Road, North Melbourne VIC 3051
Adelaide: Level 2, 14 Grote Street, Adelaide SA 5000
Email: enroll@scei.edu.au / Phone: +61 3 9602 4110
Web: www.scei.edu.au

PP70 ICT Use Policy and Procedure

PURPOSE

To outline Southern Cross Education Institute's policy towards the acceptable use of ICT, particularly concerning misuse of resources for non-educational purposes.

SCOPE

This policy applies to all staff, students and contractors of Southern Cross Education Institute.

DEFINITIONS

SCEI	Southern Cross Education Institute
Acceptable Use	Use that is consistent with the teaching, learning, assessment and administrative processes of SCEI
User	Any person accessing any of the ICT resources, including, but not limited to – staff, students, consultants, contractors, third parties, other users who are authorised by SCEI to access ICT systems and/or the network including non-SCEI ICT equipment (e.g. laptop computers, tablets) to SCEI's network.
ICT	Information and Communication Technology
ICT Resources	Any information resources provided by SCEI to assist or support teaching, learning, assessment and administrative activities. This includes, but is not limited to, physical spaces designated for teaching, study, all digital and electronic information storage, software and communication media devices, including, but not limited to, telephone, mobile phones, wireless or computer networks, computer workstation equipment including laptops, tablets, electronic email systems, internet and intranet.
ICT facilities and services	Covers all types of ICT facilities owned or leased by the SCEI, ICT services provided by SCEI and computer equipment owned or leased by users which are used to connect to SCEI networks and/or the Internet.
Collaboration Services	Refers to communication tools that allow to exchange information between individuals e.g. Skype, videoconferencing, online meeting tools, online messaging tools, voicemail, screen sharing.

POLICY

1. The Southern Cross Education Institute ICT resources are a vital resource that directly contributes to and facilitates the teaching, learning and assessment activities of students and staff. Users of the ICT resources can expect these resources to be functional within SCEI premises, and those accessible outside of SCEI premises through web login.

2. SCEI aspires to be a community characterised by a pursuit for knowledge, learning achievement, ethical practices, and academic integrity. In all its pursuits, SCEI is guided by a primary concern for equality of opportunity and equitable outcomes. This policy outlines the behavioural expectations of users of SCEI ICT resources as well as the consequences of breaching the codes of conduct as outlined.

3. ICT Use Code of Conduct

3.1. Expectations

3.1.1. SCEI requires that users of ICT Resources, facilities and services on premises or remotely to:

3.1.2. Adhere to Australian copyright laws and observe the individual terms of use when accessing materials from websites and databases;

3.1.3. Report viruses or unresolved malfunctions to IT services;

3.1.4. Use SCEI ICT Resources, facilities and services such as computers and other devices as intended;

3.1.5. Report damaged or malfunctioning ICT Resources, facilities and services to ICT services;

Melbourne: 155-161 Boundary Road, North Melbourne VIC 3051
41 Boundary Road, North Melbourne VIC 3051
Adelaide: Level 2, 14 Grote Street, Adelaide SA 5000
Email: enroll@scei.edu.au / Phone: +61 3 9602 4110
Web: www.scei.edu.au

3.1.6. Accept full responsibility for their use of ICT Resources in accordance with all relevant SCEI policies;
3.1.7. Avoid consuming an unreasonable amount of available ICT Resources (e.g. consuming an amount that would negatively impact the experience of other users);
3.1.8. Only access ICT Resources for which they are authorised;
3.1.9. Take precautions to ensure that screens displaying sensitive or critical information are not seen by unauthorised persons in public areas;
3.1.10. Be responsible for all activities originating from their accounts; and
3.1.11. Comply with the terms and conditions of any licenced third party applications.

3.2. Prohibited Behaviours

3.2.1. SCEI prohibits the conduct of:
3.2.2. Hacking internal or external computers, websites, storage facilities or other technologies;
3.2.3. Excessively downloading from the internet and/or online databases;
3.2.4. Changing or updating software unless authorised to do so;
3.2.5. Visiting pornography websites and/or displaying other obscenities;
3.2.6. Sharing personal SCEI student or staff passwords with others;
3.2.7. Loaning to others equipment that was loaned to you personally by SCEI e.g. laptop;
3.2.8. Copy, download, store or transmit material which infringes copyright, including music files, movies or videos, or pirated software;
3.2.9. Copy, download, store or transmit material available at shared drive "Quality Centre" including Training and Assessment resources, software;
3.2.10. Create or transmit any material that could reasonably be deemed offensive, obscene or indecent, intimidating or distressing (other than for approved teaching, research or incident investigation purposes);
3.2.11. Create or transmit any material that is likely to discriminate, harass or is defamatory;
3.2.12. Create or transmit any material that is confidential and for which there is no authority to transmit;
3.2.13. Avoid connecting untrusted removable storage media to SCEI mobile computing devices;
3.2.14. Use ICT resources for unauthorised commercial activities, private or financial gain to a third party;
3.2.15. Send junk-emails, for-profit messages, chain letters or unsolicited commercial emails (SPAM);
3.2.16. Subvert security by creating or installing any form of malicious software (e.g. worms, viruses, sniffers) which may affect computing or network equipment, software or data;
3.2.17. Subvert security by attempting unauthorised access to any ICT Resources.

4. Acceptable Use of the Internet

4.1. Internet connectivity is provided to SCEI users for learning, teaching, assessment and the provision of administrative purposes. All individual Internet access activity will be automatically recorded and monitored; this includes pages viewed, files and programs transferred (including user date and time of access).
4.2. Users must not access any pornographic, racially insensitive and/or similar material; and
4.3. Users must not use the Internet to attempt to gain unauthorised access to other systems.

5. Acceptable Use of Email

5.1. An email service is provided to all staff and students at SCEI.
5.2. All e-mail received, created and sent using the SCEI official email address are deemed official SCEI correspondence remain the property of the SCEI;
5.3. Personal email correspondence using the SCEI official email address is not permitted and any such emails remain the property of the SCEI;
5.4. E-mails containing sexist, racist, offensive or abusive material are not acceptable under any circumstances;
5.5. If an offensive e-mail is received it must not be distributed to others and must be reported immediately to ICT services.

Melbourne: 155-161 Boundary Road, North Melbourne VIC 3051
41 Boundary Road, North Melbourne VIC 3051
Adelaide: Level 2, 14 Grote Street, Adelaide SA 5000
Email: enroll@scei.edu.au / Phone: +61 3 9602 4110
Web: www.scei.edu.au

5.6. Users must not send e-mail which may compromise the reputation of SCEI such as harassment or chain letters, pornographic or insensitive material, or knowingly send e-mail with attachments that may contain viruses, worms, or malicious content;
5.7. Users must not knowingly open any attachments or links which are suspicious or from untrusted or unknown sources;
5.8. Users must not send e-mail impersonating someone else.

6. Acceptable Use of Phone Services

6.1. SCEI's phone systems are provided to staff for a business purposes only;
6.2. Users must not misuse phone services to make harassing, insensitive or malicious phone calls;
6.3. Calls to international numbers are not permitted unless approved by the CEO.

7. Acceptable Use of Collaboration Services

7.1. All SMS messages created and sent using the SCEI collaboration tools (e.g. TextOut) are deemed official SCEI correspondence;
7.2. Messaging is not a replacement for email and as such any formal documents or official communications should be via SCEI official email only;
7.3. Sensitive or commercial information must not be shared using messaging, online meetings, screen sharing or video conferencing services as the services are not designed for such purposes;
7.4. Users must not use messaging, screen sharing or online meetings for sharing personal, malicious or copyright file attachments that are not directly related their employment or studies;
7.5. Users must not use collaboration services which may compromise the reputation of the SCEI such as harassment, pornographic or insensitive material;
7.6. Users are reminded to be mindful when using available desktop sharing functionality not to expose sensitive or SCEI commercial information;
7.7. All use of collaborative services are monitored and recorded. Information is stored and archived to meet SCEI record management requirements.

8. Breaches to this Policy

8.1. Breaches of any element of this policy is unacceptable and may result in penalties or disciplinary action depending on the offence or offences that occurred.
8.2. Disciplinary action will be in accordance with the:
8.2.1. PP79 Student Rules Policy
8.2.2. PP99 Student Misconduct Policy and Procedure

RELATED DOCUMENTS

PP79 Student Rules Policy
PP99 Student Misconduct Policy and Procedure
PP85 Email and SMS Policy and Procedure

LEGISLATIVE CONTEXT

NIL

RESPONSIBILITIES

IT Manager
Responsible for monitoring user compliance with this policy and investigating and reporting breaches of this policy.

Melbourne: 155-161 Boundary Road, North Melbourne VIC 3051
41 Boundary Road, North Melbourne VIC 3051
Adelaide: Level 2, 14 Grote Street, Adelaide SA 5000
Email: enroll@scei.edu.au / Phone: +61 3 9602 4110
Web: www.scei.edu.au

Managers

Responsible for reporting any security incidents or breaches of this policy by staff under their supervision to the IT Manager.

Users

Responsible for reporting any security incidents and breaches of this policy to IT Manager or their direct line manager.

Author	Compliance Manager
Approved by	CEO
Effective date	14/03/2017
Version	3.2
Review date	November 2018