Use of ICT (Information and Communications Technology) Policy and Procedure

Purpose

1. This Policy sets the Australian International Institute of Higher Education's ('the Institute') expectations with regard to students' use of the Institute's information and communications technology (ICT) systems and resources.

Scope

2. This Policy applies to:
   a) all students
   b) all information technology tools and resources as outlined in the ***Definitions.***
3. Arrangements for the management of the Institute's technology tools and resources, including access, support and security, are outlined in the *ICT Management Plan*.

Definitions

4. For the purposes of this Policy:
   a) ***Information and Communications Technology (ICT)*** means technological tools and resources used to transmit, store, create, share or exchange information that is provided by the Institute, including email accounts, student portal, learning management system, online library collection, access to the internet, and general and specialist software.

Policy

Principles

5. The Institute is committed to providing a safe, respectful, cooperative and productive educational environment. The Institute gives students access to IT systems and resources to support their studies at the Institute, including for the sharing of subject information, group work but also for general interactions between students.
6. The Institute aims to safeguard the privacy, availability, integrity, security, safety, and usability of ICT systems and resources. The achievement of these aims is supported by the collaboration of students who are expected to use the ICT systems and resources provided by the Institute for the purpose of their studies, responsibly, safely, securely, and lawfully.
7. The provisions of the Institute's *Student Code of Conduct* apply to the use of ICT systems and resources. This Policy complements, and is not a substitute for, the Student Code of Conduct. A breach of the principles for the use of ICT may lead to disciplinary action, up to cancellation of enrolment.

Proper purpose

8. Students should use ICT systems and resources for the purpose of their studies at the Institute. This includes:
   a) limiting personal use (e.g. communicating with family)
   b) not engaging in commercial activity.

Responsible use

9. Students must use ICT systems and resources responsibly. This includes:
   a) not causing damage to the systems and resources
   b) not interfering with their normal functioning
   c) reporting any dysfunction to the Institute staff.

Safety

10. Students must not pose a risk to their, or others', safety while using ICT systems and resources. This includes:
    a) displaying the same standards of behaviour online as on campus
    b) conducting themselves in a respectful manner
    c) not downloading, uploading, or publishing harmful content
    d) protecting their own, and others', privacy.

Security

11. Students must preserve the confidentiality of their access details. This includes:
    a) not sharing their login details with anyone
    b) regularly changing their password
    c) seeking guidance from Student Services if they believe their access details may have been compromised.
12. Students must not access, or attempt to access, ICT systems and resources without authorisation from the Institute.
13. Students must not compromise the security of ICT systems and resources. This includes not downloading, uploading, or using unauthorised software.

Lawfulness

14. Students must not handle any unlawful material. This includes not downloading, uploading, or publishing illegal content.
15. Students must not breach intellectual property rights. This includes:
    a) appropriately identifying sources when reproducing content; and
    b) not downloading, uploading, or using illegally sourced software or content.

Bring Your Own Device (BYOD)

16. The Institute recognises that students may use personal devices such as laptops, tablets, and smartphones on-campus and off-campus to access the Institute's ICT systems and resources for their studies, provided that such use aligns with the principles of responsible, safe, and lawful ICT usage. While students are permitted to use their own devices, they must ensure that their devices comply with the Institute's security and usage guidelines. This includes

maintaining up-to-date antivirus software, using secure passwords, and ensuring their devices do not pose security risks to the Institute's ICT infrastructure.

17. The Institute reserves the right to restrict or deny access to its ICT systems if a student's device is found to compromise security, functionality, or compliance with this Policy.
18. The Institute is not responsible for the maintenance, security, or technical support of students' personal devices.

Procedure

ICT risk management

19. The Institute adopts a risk-based approach to the management of ICT systems and resources and implements a range of controls for preventing and mitigating risks to student and business outcomes, including safety, academic integrity, and availability of services.
20. Use of ICT systems and resources is monitored by the Institute.
21. The Institute may suspend or cancel student access to ICT systems and resources on an individual or general basis without notice.
22. Where there is reason to believe a criminal offence may have been committed, the Institute will report the incident to Queensland Police.
23. The Institute provides students with guidance on the safe and secure use of ICT systems during orientation and issues regular reminders on online safety.
24. The Institute provides support services relevant to the use of ICT systems and resources, including introduction to the learning management system, use of ICT facilities on campus, and support services for online incidents.
25. The Institute will investigate all reported incidents, hazards, or near misses in accordance with the applicable policy, including the *Work Health and Safety Policy, Academic Integrity Policy*, and the *Student Misconduct Policy*.

BOYD procedures

26. Students intending to use their personal devices to access the Institute's ICT systems and resources must ensure their devices comply with minimum security requirements, including:
    a) The device must have up-to-date antivirus and anti-malware protection installed.
    b) The device must be password-protected and have appropriate security settings enabled to prevent unauthorised access.
    c) Students must ensure that their device operating systems and software are regularly updated to protect against security vulnerabilities.
    d) Students must use secure network connections, such as the Institute's designated Wi-Fi network, and avoid unsecured public networks when accessing Institute resources.
27. Students experiencing connectivity or access issues with their personal devices may seek guidance from Student Services. The Institute's IT team may provide students with guidance on configuring their devices for secure access but is not responsible for the maintenance or troubleshooting of personal devices.
28. If a student's device is identified as a security risk or found to be interfering with the Institute's ICT systems or violating this policy, the Institute may temporarily or permanently restrict access until the issue is resolved.
29. Students must report any suspected security breaches, malware infections, or unauthorised access attempts involving their personal devices to Student Services or the ICT Manager immediately.

30. The Institute reserves the right to conduct periodic security audits and recommend necessary actions to ensure compliance with this Policy.

Monitoring and improvement

31. The Institute collects data on the use of ICT by students. Student feedback is sought on their experience of ICT systems and resources at the Institute, including online safety, security, system integrity, usability, and support services.
32. The Institute uses the collected data to monitor trends in breaches of the principles for the use of ICT and breaches of ICT security.
33. The Institute will improve its strategies for the acceptable use of ICT based on the collected data.
34. The Institute will benchmark its performance against relevant industry data and will establish targets as appropriate.
35. The Governing Council receives an annual report on the adequacy and effectiveness of its strategies.

Appeals

36. A student may appeal against a decision made under this Policy under the provisions outlined in the *Student Appeals Policy and Procedure*.

Records

37. Records of any breaches of this Policy will be maintained according to the provisions of the *Student Misconduct Policy and Procedure*.

Responsibilities

38. Students are responsible for:
    a) abiding by the principles included in this Policy and taking active steps to prevent inadvertent breaches
    b) reporting any online incident, hazard, or near-miss to Student Services or in accordance with the relevant policy as applicable.
39. ICT Manager is responsible for:
    a) Supporting Course Coordinators in maintaining the Learning Management System, Marketing and Admission Officer in maintaining the Institute's website, Student Services Manager in maintaining the Student Management System and records management, Librarian in maintaining the Library Management System, and the CEO in maintaining other required applications
    b) maintaining ICT infrastructures on all campuses.
40. The Audit and Risk Committee is responsible for including ICT resources in its regular monitoring and risk management activities.
41. The Chief Executive Officer is responsible for:
    a) coordinating risk management activities for the use of ICT by students through the Executive Management Team, in particular, identification of the Institute's and students' exposure to safety, privacy, and interference risks
    b) arranging an orientation module on acceptable use of ICT and regular evidence-based educational campaigns on online safety and security.

Associated information

Approving body	Governing Council
Date approved	23 October 2020
Date of effect	Commencement of operation
Scheduled review	Two years from when policy commences
Current version approval date	10/02/2025
Next review date	10/02/2027
Policy owner	Chief Executive Officer
Policy contact	Chief Executive Officer
Related AIIHE Documents	Academic Freedom Policy Student Academic Integrity Policy and Procedure Campus Facilities and Security Policy and Procedure Critical Incident and Emergency Management Plan Facilities and Resources Review Policy and Procedure ICT Management Plan Learning Technologies Policy and Procedure Student Code of Conduct Student Equity and Diversity Policy and Procedure Student Appeals Policy and Procedure Student Misconduct Policy and Procedure Student Support Framework Work Health and Safety Policy and Procedure
Higher Education Standards Framework (Threshold Standards) 2021 (Cth)	Standard 2.1, ss 2–3 Standard 2.3, ss 2–5 Standard 3.3, ss 1–4 Standard 5.2, ss 1–3 Standard 7.3, ss 3
Other related external instruments/documents	**Related Legislation** • Tertiary Education Quality and Standards Agency Act 2011 (Cth) • Education Services for Overseas Students Act 2000 (Cth) • National Code of Practice for Providers of Education and Training to Overseas Students 2018 (Cth) • Cybercrime Act 2001 (Cth) • Copyright Act 1968 (Cth) • Spam Act 2003 (Cth) **Good Practice Documents** • TEQSA Guidance Note: Staffing, Learning Resources and Educational Support, Version 1.3 • TEQSA Guidance Note: Wellbeing and Safety, Version 1.2

Document history

Version	Author	Changes	Approval Date
1.0	Not applicable	Original version	23 October 2020
1.1	Compliance Officer	Reviewed to align with the HESF 2021, the responsibilities section was strengthened by adding the applicable key position, and the footer was updated with current addresses.	15 July 2024
1.2	Compliance Officer	Policies and procedures related to Bring Your Own Device (BYOD) have been incorporated	10 February 2025

N.B. The document is uncontrolled when printed! The current version of this document is maintained on the AIIHE website at www.aiihe.edu.au.