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

Approving body	Governing Board (GB)
Date approved	27 Feb 2025
Date of effect	Commencement of operation
Next scheduled review	Two years from when policy commences
Policy owner	Chief Executive Officer (CEO)
Policy contact	Chief Executive Officer (CEO)
Related Documents	Student Code of Conduct Student Grievance Policy and Procedure Student Appeals Policy and Procedure Student Misconduct Policy and Procedure ICT and Cyber Security Management Policy and Procedure

Purpose

1. This Policy establishes **Zenith Innovation Institute's** (**Zenith / the Institute**) expectations regarding students' use of Zenith / the Institute's information and communications technology (**ICT**) systems and resources.

Scope

2. This Policy applies to:

    (a) all students, whether on-campus, off-campus, or using personal devices to access Zenith's ICT systems; and

    (b) All information technology tools and resources made available to students, including but not limited to.

    (i) Email accounts, student portals, learning management system (LMS), student management system (SMS), library collections (including eBooks), teaching software and IT systems.

    (ii) On-campus and remote access to Zenith's ICT infrastructure, including Wi-Fi, VPN, and digital platforms

    (iii) Third-party ICT systems and equipment used for workshops, work-integrated learning (WIL), and external academic partnerships

    (iv) Any ICT resources used for assessments, including online quizzes, forums, and student authentication measures.

3.   Arrangements for the management of the Institute's technology tools and resources, including for access, support and security are outlined in the ICT Management Policy.

Policy

General ICT Usage Expectations

4.   The Institute is committed to providing a safe, respectful, and cooperative digital learning environment. Students are granted access to ICT systems and resources, including free Wi-Fi while on campus, to support their studies.

5.   The privacy, security, availability, and integrity of Zenith's ICT systems will be protected, and students are expected to use these systems responsibly and lawfully.

6.   Any misuse of ICT resources may result in disciplinary action, including suspension or termination of access.

Principles

7.   The principles applying to the use of the Institute's ICT systems and resources are:

   (a)   **Bring Your Own Device** – Students can bring their own device to campus but when using the Institute's wi-fi, will abide by the principles of this Policy and Procedure;

   (b)   **Proper purpose** – ICT systems and resources must be used primarily for academic purposes. Limited personal use is permitted, provided it does not interfere with academic responsibilities or breach this Policy;

   (c)   **Responsible use** – The Institute's ICT systems and resources should be used responsibly and not be damaged or interfered with. If the ICT systems and resources are not functioning properly, students should report this to the IT Support Team;

   (d)   **Safety** – Students must not pose a risk to their own safety, or those of others, while using the Institute's ICT systems and resources, or those of the Institute's partner institutions. This includes:

      (i)   displaying the same standards of behaviour online as on campus;

      (ii)   conducting themselves in a respectful manner;

      (iii) not downloading, uploading, or publishing harmful content; and

      (iv)   protecting their own, and others', privacy;

   (e)   **Security** - Students must not compromise the security of ICT systems and resources, including downloading, uploading, or using unauthorised software:

      (i)   Students must protect their access details from others, including:

         (A)   not sharing login details with others;

         (B)   attempt to impersonate another student when accessing ICT systems;

         (C)   Provide false or misleading information when completing assessments, quizzes, or online activities;

         (D)   changing their password on a regular basis; and

         (E)   seeking guidance from Student Services if they believe their access details may have been compromised; and

   (f)   **Lawfulness** – including but not limited to:

      (i)   Students must not handle any unlawful material. This includes not downloading, uploading, or publishing illegal content;

      (ii)   Students must not breach intellectual property rights by downloading, uploading or using illegally sourced software or content;

(iii)   Downloading, uploading, or sharing illegal content (e.g., copyrighted material, offensive media);

(iv)   Breaching intellectual property rights (e.g., using unauthorised software);

(v)   Cyberbullying, harassment, or sharing explicit/abusive material; and

(vi)   Engaging in fraudulent activities, including identity theft.

Any illegal activity using Zenith's ICT systems (e.g., emails, VPN, networks) may be reported to the relevant authorities for prosecution. Zenith will fully cooperate with law enforcement agencies.

(g)   **Respect for Equipment and Facilities** – Students must respect and properly use all ICT equipment and spaces, including:

(i)   Computer labs, networked devices, and digital classrooms;

(ii)   Equipment used in IT-related workshops or work-integrated learning (WIL) programs; and

(iii)   Any third-party ICT systems used during external placements.

Procedure

ICT risk management

8.   During orientation, students will be provided with guidance on the appropriate and safe use of the Institute's ICT systems and resources, including ensuring students are aware of the content of this Policy and Procedure.

9.   If there has been a breach of the Principles outlined above, above, the Institute may suspend or cancel the student's access to the ICT systems and resources.

10.   The Institute will provide students with training and support in the use of the Institute's ICT systems and resources, including an introduction on the Institute's learning management system and student portal.

Monitoring and improvement

11.   The Institute will collect data on student feedback about their use of the Institute's ICT systems and resources, including security and integrity of the system, and their usability.

12.   Feedback will be used to improve the ICT systems and resources for students. Feedback on ICT usability, security, and system integrity will be collected through:

(i)   Surveys, IT helpdesk reports, and security incident reviews.

(ii)   Continuous improvement initiatives to enhance ICT accessibility and performance

Appeals

13.   A student may appeal against a decision made under this Policy under the provisions outlined in the Student Grievance Policy and Procedure and if dissatisfied with the outcome, appeal under the provisions of the Student Appeals Policy and Procedure.

Responsibilities

14.   Students are responsible for:

(a)   abiding by the principles set out in this Policy and Procedure; and

(b)   reporting any online incident to the relevant staff.

Definitions

15.   There are no definitions for this Policy.

Version History

Version	Changes	Approval Body	Approval Date
1.0	New Policy	Governing Board (GB)	19 Sep 2024
1.1	Point 2 a) added "whether on-campus, off-campus, or using personal devices to access Zenith's ICT systems" and elaborated the scope. Reworded 7 b) to "ICT systems and resources must be used primarily for academic purposes. Limited personal use is permitted, provided it does not interfere with academic responsibilities or breach this Policy" Point 7 c) replaced "relevant staff" with "IT Support Team" Under 7 e) Security added "attempt to impersonate another student when accessing ICT systems;" and "Provide false or misleading information when completing assessments, quizzes, or online activities" Under 7 f) added "but not limited to" then added three new points Added 7 g) Respect for Equipment and Facilities Point 12 outlined how feedback will be collected.	GB	27 Feb 2025