Provision and Acceptable Use of IT Resources Policy

1. Purpose and Scope

The King's Own Institute (KOI) provides and uses information technology (IT) resources throughout all its activities. This policy outlines the access standards, and the acceptable and appropriate use of IT resources, sets out the responsibilities of all authorised users, and describes the penalties for policy breaches.

KOI provides access to IT resources for authorised users and takes steps to prevent inappropriate use of these resources. This policy applies to all students, staff, contractors, affiliates, and visitors who have access to KOI IT resources.

2. Related Documents

This Policy should be read in conjunction with KOI's other relevant policies and procedures, including:

- IT Disaster Recovery Policy
- Bring Your Own Device (BYOD) Policy

3. Definitions

Authorised user: Any enrolled student, staff member, or approved associate of KOI who has been granted access to use IT resources for purposes related to their relationship with KOI.

4. Policy

KOI grants access to its IT resources to all authorised users for the purpose of pursuing and advancing its business and educational goals. As a condition for making use of the IT resources, KOI requires that all authorised users agree to the conditions set forth in this policy.

All KOI IT resources, including named email accounts provided to authorised users for their study or work, are and remain the property of KOI. While authorised users may make incidental personal use of the IT resources, such use must be legal and must not breach KOI policies. Excessive or illegal downloading is prohibited.

The use of Generative AI tools and services must comply with KOI's academic integrity standards and intellectual property rights. While KOI recognises the potential educational value of GenAI tools, their use must be appropriately disclosed when required for academic work. Using GenAI to impersonate others, generate misleading content, or circumvent security measures is strictly prohibited. Users must be aware that GenAI outputs may contain inaccuracies, biases, or copyrighted content. All GenAI-assisted work must be properly reviewed, fact-checked, and attributed according to KOI's academic standards.

In cases where an authorised user breaches the terms of this policy, their access may be restricted or revoked. Student breaches will be treated as non-academic misconduct. Depending on their nature and seriousness, breaches may be reported to relevant authorities or police for appropriate action.

Any person who observes breaches of this policy should report them to the IT Team immediately. All breach reports will be treated confidentially. Complaints resulting from alleged breaches will be managed according to the established procedures outlined in the Complaints and Appeals Policy and the Complaints Policy (for staff).

The Director of IT holds the authority to temporarily deny or restrict access to IT resources, including

email, when necessary to prevent policy or legal breaches, investigate potential breaches, or mitigate threats or risks to KOI and its IT resources.

5. Principles

Information technology at KOI should be used effectively and efficiently to enhance educational quality and the student learning experience. The scope of this policy encompasses all KOI owned and imaged computers, including laptops and netbooks, data storage systems, printers, and photocopiers.

IT Services maintains responsibility and accountability for the strategic management, development, and support of information technology across KOI. This includes providing related documentation, services, and training to all staff and students. KOI promotes a transparent and collegial approach that recognises the role and responsibilities of all stakeholders in the development and adoption of information technology.

Innovation in information technology is actively encouraged at KOI. Proposals for the adoption of added information technology can be advanced and developed in any area of the institution.

6. Roles and Responsibilities

Director of IT: The Director of IT bears primary responsibility for the implementation and operation of this policy. In this capacity, the Director will provide regular reports to the CEO and President for communication to the Council regarding IT developments, IT security, and IT breaches.

Authorised users: Authorised users must fulfil several key responsibilities in their use of KOI IT resources. They must comply with all KOI policies and implement strong security practices, including choosing and periodically changing strong passwords, enabling multi-factor authentication, and maintaining password confidentiality. Users must never share their passwords or request passwords from others.

Authorised users are prohibited from attempting to undermine the confidentiality, integrity, or availability of IT Resources without appropriate approval. They must not download copyrighted material, access torrent sites, use IT resources for private commercial enterprises or personal gain, or engage in excessive personal use of resources.

Furthermore, authorised users must avoid any activities that might disrupt other users, damage KOI's reputation, compromise personal information, or create a hostile environment. This includes refraining from threatening, bullying, harassing, or discriminatory behaviour, avoiding the distribution of offensive material, and preventing unauthorised access attempts to systems or data.

Authorised users must not use GenAI tools to generate content that impersonates KOI staff, students, or systems; attempt to circumvent IT security measures or generate malicious code; create deceptive or fraudulent communications; and/or automate unauthorised access to KOI resources. Authorised users should verify the accuracy and appropriateness of GenAI-generated content before use in official KOI communications or academic work; and understand the limitations and potential risks of GenAI tools in their specific use context.

7. Associated Information

KOI provides a comprehensive suite of computing facilities to support its educational mission. These services include a staffed IT Service Desk during business hours, access to Google Workspace and MS Office 365 education accounts, campus-wide Wi-Fi systems, and various academic and administrative information

systems. Users also have access to standard software suites, printing and scanning facilities, and KOI computers and network storage, with access levels appropriately designated for different user groups.

Access management follows specific timelines and procedures. Student access becomes available 24 hours after enrolment and terminates upon course completion or departure from KOI. Email accounts for graduated students remain active for 180 days after completion, while accounts for withdrawn students are disabled 180 days after their withdrawal.

For users employing their own devices (BYOD), specific security responsibilities apply. Users must take active measures to prevent theft or loss of digital information, maintain appropriate information confidentiality, and promptly report any loss of devices containing KOI data. All BYOD usage must comply with the detailed requirements outlined in the BYOD policy available on the KOI website.

Use of Generative AI Tools: KOI recognises that GenAI tools may be used to support educational and administrative activities. However, such use must align with KOI's academic policies and IT security requirements. Users must exercise caution when inputting KOI data into external GenAI services and ensure no confidential or sensitive information is disclosed. KOI reserves the right to restrict access to specific GenAI services that pose security or integrity risks to its IT resources.

Security and monitoring procedures are integral to protecting KOI's IT resources. Users bear responsibility for the security of all data accessed under their credentials. The IT Team conducts routine monitoring of computer activities, and KOI maintains the right to monitor network usage and materials. The institution commits to responding promptly to any security breaches.

Document Control

Policy Title:	Provision and Acceptable Use of IT Resources Policy
Policy Owner	Director of IT
Policy Approver	AIBM Council
Policy version date	29 August 2025 Version 1.5
Date of approval	29 August 2025
Date of implementation	29 August 2025
Date of next review	29 August 2026
Changes in this version	Minor changes in this version included adding requirements for users to verify GenAI output accuracy and understand GenAI limitations before using AI-generated content in official KOI communications or academic work.