Bring Your Own Device (BYOD) Policy

1. Purpose and Scope

1.1 Purpose

This policy establishes guidelines and requirements for the use of personally owned devices to access King's Own Institute (KOI) IT resources. The policy aims to ensure the security of KOI data and systems while enabling flexible device usage that enhances productivity and learning experiences for authorised users.

1.2 Scope

This policy applies to all authorised users of KOI IT resources, including staff, contractors, affiliates, and visitors who use their personal devices to access KOI systems, networks, or data. The policy covers all personal devices used to access, store, or process KOI information and resources, whether on campus or remotely.

2. Related Documents

This policy should be read in conjunction with the following KOI documents:

- Provision and Acceptable Use of IT Resources Policy
- Staff Complaints and Appeals Policy
- Staff Code of Conduct
- Privacy Policy

3. Definitions

For the purposes of this policy:

BYOD (Bring Your Own Device) refers to the practice of using personally owned devices to access organisational resources. This includes any computing device not provided by KOI that is used to access KOI systems or data at all KOI campus locations.

Authorised Users are all staff and approved associates of KOI who have been granted access to KOI IT resources through proper authorisation channels.

Personal Devices encompasses any mobile device, laptop, tablet, or other computing device owned by the user rather than provided by KOI. This includes but is not limited to smartphones, personal laptops, tablets, and other mobile computing devices.

KOI Data includes any information created, stored, or transmitted using KOI IT resources or on behalf of KOI, regardless of its format or location.

IT Resources refers to KOI's network infrastructure, systems, applications, and services that are made accessible to authorised users for educational and administrative purposes.

4. Policy

4.1 Device Requirements

All personal devices used to access KOI IT resources must meet minimum security standards to protect KOI's systems and data. These requirements include maintaining current and updated anti-virus software on the device, ensuring operating system security patches are promptly installed, implementing secure

password protection, and enabling automatic screen locking features. Users must configure their devices to meet these requirements before accessing KOI resources.

4.2 Network Access and Usage

KOI provides network access for personal devices through its Wi-Fi infrastructure. Users may connect their devices to access authorised KOI systems and services, including email and learning management systems. When accessing KOI resources, users must comply with all relevant IT policies and maintain appropriate security measures. Network access is provided primarily for educational and work-related purposes, with incidental personal use permitted within reasonable limits.

4.3 Data Protection

Users have a responsibility to protect KOI data accessed or stored on their personal devices. This includes maintaining the confidentiality of institutional information, preventing unauthorised access to KOI systems, and ensuring proper handling of sensitive data. Users must not download or store sensitive KOI data on personal devices without explicit authorisation and must remove all KOI data when it is no longer needed or upon termination of their relationship with KOI.

Users must exercise caution when using GenAI tools on personal devices that access KOI data. KOI data must not be uploaded to external GenAI services without explicit authorization. Users should be aware that GenAI platforms may retain, analyse, or use uploaded data for training purposes, potentially compromising KOI's confidentiality.**4.4 Security Incidents**

Security incidents involving personal devices must be reported immediately to the Director of IT. This includes lost or stolen devices containing KOI data, suspected security breaches, unauthorised access attempts, malware infections that could affect KOI resources, inadvertent disclosure of KOI data to GenAI platforms or services, and suspected compromise of credentials through GenAI-assisted phishing or social engineering attacks. Prompt reporting enables appropriate response measures to protect KOI's systems and data from potential compromise.

4.5 Support Services

IT Services provides defined support for personal devices used to access KOI resources. Support includes assistance with network connectivity and access to KOI systems. However, IT Services does not provide hardware support, personal software installation, personal data backup, or support for personal applications. Users are responsible for maintaining their own devices and seeking external support for device-specific issues.

4.6 Compliance and Enforcement

KOI maintains the right to protect its resources through appropriate measures, including denying or revoking access to KOI resources, removing KOI data from personal devices, monitoring network traffic and device access, and investigating potential policy violations. Non-compliance with this policy may result in disciplinary action in accordance with relevant KOI policies.

4.7 GenAI Usage on Personal Devices:

When using GenAI tools on personal devices to support KOI-related activities, users must: avoid inputting confidential KOI information, student data, or proprietary content; use only approved GenAI tools as specified in the Provision and Acceptable Use Policy; ensure appropriate disclosure when GenAI is used in academic or administrative work; and report any suspected data breaches involving GenAI platforms immediately

5. Principles

This policy is guided by the following principles:

The use of personal devices must not compromise the security, integrity, or confidentiality of KOI's data and systems. While KOI encourages the use of personal devices to enhance productivity and learning experiences, such use must be balanced against security requirements.

Access to KOI IT resources through personal devices is provided as a privilege, not a right. This privilege may be revoked if users fail to comply with policy requirements or engage in activities that threaten the security of KOI systems.

Users bear primary responsibility for the security and appropriate use of their personal devices. This includes maintaining device security, protecting access credentials, and ensuring appropriate handling of KOI data.

KOI supports flexible learning and working arrangements through the accommodation of personal devices where such use enhances educational and administrative outcomes.

All BYO devices will be subject to onboarding/offboarding procedures. As part of the onboarding process, the authorised user needs to agree and sign the "BYOD Agreement" document (under development). KOI reserves the right to delete/wipe the KOI Data in the device if the device is lost or is offboarded.

6. Roles and Responsibilities

6.1 Director of IT

The Director of IT holds primary responsibility for implementing and overseeing the BYOD policy. This includes managing security incidents and policy breaches, providing regular reports to the CEO/Dean and President regarding BYOD implementation and effectiveness, and ensuring the policy remains current with technological developments and institutional needs.

6.2 IT Services

IT Services plays a crucial role in supporting the BYOD environment. The department provides approved support services, monitors network access and security, implements technical controls to protect KOI resources, and assists with investigating security incidents involving personal devices.

6.3 Users

All users of personal devices must comply with security requirements, promptly report security incidents, maintain their devices in secure condition, and protect any KOI data accessed through their devices. Users are expected to exercise good judgment in their use of personal devices and follow all applicable policies and procedures.

6.4 Academic Board

The Academic Board reviews and recommends approval of the BYOD policy and oversees its academic implications. The Board ensures that the policy supports educational objectives while maintaining appropriate security standards.

6.5 AIBM Council

The AIBM Council approves the BYOD policy and major revisions, providing governance oversight of the BYOD program. The AIBM Council ensures alignment with KOI's strategic objectives and risk management framework.

7. Associated Information

7.1 Implementation

Implementation of this policy occurs through a combination of technical controls on network access, user education and awareness programs, regular security monitoring, and incident response procedures. IT Services maintains detailed procedures for implementing policy requirements and responding to security incidents.

7.2 Monitoring and Review

The policy undergoes review every three years or more frequently if required by changes in technology or institutional needs. Regular compliance monitoring and annual security assessments help ensure policy effectiveness. Security incidents are tracked and reported to identify trends and areas requiring additional controls.

Document Control

Policy title	Bring Your Own Device (BYOD) Policy
Policy owner	Director of IT
Policy approver	AIBM Council on the recommendation of the Academic Board and Audit and Risk Committee
Policy version date	29 August 2025 Version 1.1
Date of approval	29 August 2025
Date of implementation	29 August 2025
Date of next review	29 August 2026
Changes in this version	The main changes in this version include prohibiting users from uploading KOI data to external GenAI services without authorisation and requiring them to report any inadvertent data disclosure to GenAI platforms as security incidents. Users would be required to avoid inputting confidential KOI information into GenAI tools on their personal devices, use only approved GenAI tools, and ensure proper disclosure when GenAI assists with KOI-related work. The additions also emphasise that GenAI platforms may retain uploaded data for training purposes, creating potential confidentiality risks for institutional information.