BRING YOUR OWN DEVICE (BYOD)

POLICY NUMBER: ADM-BYOD
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: VICE PRESIDENT-ADMINISTRATION & FINANCE
RESPONSIBLE OFFICE: INFORMATION TECH. (IT) / CHIEF INFORMATION SECURITY OFFICER
EFFECTIVE DATE: UPON PRESIDENTIAL APPROVAL – 2/8/2024
NEXT REVIEW DATE: PRESIDENTIAL APPROVAL PLUS FOUR (4) YEARS – 2/8/2028
SUPERSEDES POLICY DATED: N/A – NEW POLICY
BOARD OF REGENTS REPORTING (CHECK ONE):
☐ PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM)
☒ PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

The purpose of this Bring Your Own Device (BYOD) policy is to define the acceptable use of personal electronic devices for University-related purposes at Northern Kentucky University (NKU). This policy is intended to enhance productivity and collaboration while maintaining the security and integrity of University data and networks.

NKU supports the use of personal devices for University-related activities and encourages the responsible use of these devices while maintaining security, confidentiality, and the appropriate use of University resources.

II. ENTITIES AFFECTED

This policy applies to all faculty, staff, and students who use personal electronic devices to access or use NKU networks, systems, or resources.

III. DEFINITIONS

Personal Electronic Devices: Any electronic device owned by an individual, including but not limited to smartphones, tablets, laptops, and wearable technology.

University Data: Any data owned or managed by NKU, including but not limited to student records, financial information, and intellectual property.

University Networks: The wired and wireless networks provided by NKU for the purpose of accessing University resources, including the internet.

IV. PERSONAL ELECTRONIC DEVICE REQUIREMENTS

- Personal electronic devices must maintain good security practices including keeping the device's operating system up-to-date, using active and current antivirus software, and having regular security updates installed.
- Personal electronic devices must be password-protected, with strong passwords or biometric authentication.
- Individuals must report lost or stolen personal electronic devices used for access or storage of University data to NKU's IT Help Desk immediately.

V. ACCEPTABLE USES

- Personal electronic devices may be used for University-related activities, including accessing NKU email, calendars, documents, and learning management systems.
- Personal electronic devices may be used to access University networks and resources, provided they meet the requirements listed in section IV above.
- Personal electronic devices may be connected to the University's wireless network but may not be connected directly to the University's wired network without prior authorization.
- Individuals must erase the storage of all confidential and private University data before reselling, gifting, or recycling a personal electronic device.

VI. UNACCEPTABLE USES

- Individuals must not store confidential or private University data on personal electronic devices, including, but not limited to, personally identifiable information regarding students and research subjects. Exceptions may be approved only in extraordinary circumstances by the Chief Information Security Officer in collaboration with the relevant administrators and supervisors.
- When on NKU networks, personal electronic devices must not be used to bypass University network security measures or restrictions.
- Personal electronic devices must not be used to engage in activities that violate NKU policies or local, state, or federal laws.

VII. SUPPORT AND MAINTENANCE

- Individuals are responsible for the maintenance, updates, and troubleshooting of their personal electronic devices.
- NKU IT may provide limited support for connecting personal electronic devices to University resources and may assist in securing and/or removing data from a device if lost or stolen.

VIII. LIABILITY

- NKU is not responsible for any loss or damage to personal electronic devices resulting from University-related activities.
- Other than NKU preapproved arrangements, individuals are responsible for any costs associated with the use of personal electronic devices, including data charges and device repairs.

IX. POLICY COMPLIANCE

- Individuals who violate this policy may be subject to disciplinary action, up to and including termination of employment or expulsion for students, in accordance with processes described in NKU policies, codes, and handbooks.
- NKU IT/Information Security may block or disconnect devices that pose a security risk or violate this policy.

X. REFERENCES AND RELATED MATERIALS

RELATED POLICIES

Acceptable Use

Information Security

Data Governance and Security

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
New Policy	February 8, 2024

BRING YOUR OWN DEVICE (BYOD)

PRESIDENTIAL APPROVAL

PRESIDENT

Signature Cady Short-Thompson *Date* 2/8/24

Cady Short-Thompson

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☐ This policy was forwarded to the Board of Regents on the ***Presidential Report (information only)***.
Date of Board of Regents meeting at which this policy was reported: _____/_____/_____.

☐ This policy was forwarded to the Board of Regents as a ***Presidential Recommendation (consent agenda/voting item)***.

- ☐ The Board of Regents approved this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing approval of policy.)
- ☐ The Board of Regents rejected this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

SECRETARY TO THE BOARD OF REGENTS

Signature *Date*

Tammy Knochelmann