ACCEPTABLE USE

POLICY NUMBER: IT-ACCEPTUSE
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: VICE PRESIDENT-ADMINSTRATION & FINANCE
RESPONSIBLE OFFICE: INFORMATION TECHNOLOGY (IT) / CHIEF INFORMATION OFFICER (CIO)
EFFECTIVE DATE: UPON PRESIDENTIAL APPROVAL – 9/1/2008
MOST RECENT REVISION: 2/8/2024
NEXT REVIEW DATE: PREVIOUS REVISION PLUS FOUR (4) YEARS – 2/8/2028
BOARD OF REGENTS REPORTING (CHECK ONE):
☐ PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM)
☒ PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

The purpose of this policy is to outline the acceptable use of technology resources at Northern Kentucky University (NKU) to promote a productive, secure, and respectful technology environment that supports the University's mission and goals. This policy outlines the responsibilities of all individuals, including students, faculty, staff, and visitors, who access and use NKU's technology resources.

Technology resources are provided for the purpose of supporting NKU's educational, research, and administrative activities. Individuals are expected to use these resources in a manner that is consistent with these purposes and in compliance with all applicable laws, regulations, and University policies.

All individuals accessing and/or using technology resources MUST:

(a) Protect their account credentials, including usernames and passwords, and not share them with others.

(b) Use technology resources in a manner that does not disrupt or interfere with the work of others, the University's mission, or the performance or integrity of technology resources.

(c) Report any security incidents or observed violations of this policy to NKU IT Help Desk.

(d) Maintain the confidentiality of data stored on NKU technology resources in the manner required by law or University policy.

(e) Comply with all applicable federal, state, and local laws, as well as University policies and procedures

Individuals MUST NOT engage in the following activities:

(a) Unauthorized access or use of any technology resources, including attempting to bypass security measures or gain access to another individual's account.

(b) Intentionally or negligently introducing malicious software (e.g., viruses, worms, or Trojan horses) into the University's technology resources.

(c) Unauthorized copying, distribution, or sharing of copyrighted materials, including software, music, movies, or other digital content, or engaging in other copyright infringement.

(d) Engaging in activities that interfere with the normal operation of the University's technology resources or the ability of others to use these resources effectively.

(e) Using technology resources for personal gain or non-University commercial purposes, except when such use is for purposes related to traditional works or as part of an approved conflict-of-interest management plan.

(f) Using technology resources, including email, social media, or other digital communication channels in violation of University policies regarding harassment or discrimination.

(g) Misrepresenting oneself or the University in electronic communications, including forging email headers or using another individual's identity.

(h) Using technology resources to engage in illegal activities.

Limited incidental personal use of NKU technology resources is permitted, as determined by the appropriate supervisor. Such use must comply with University policies.

II. ENTITIES AFFECTED

This policy applies to all individuals who use NKU technology resources, including students, faculty, staff, contractors, visitors, and any other individuals who access or use NKU's technology resources, regardless of the location from which they are accessed.

III. AUTHORITY

Individuals must report any observed violation of this policy to NKU's IT Help Desk or Information Security. Individuals must also cooperate with any investigation related to violations of this policy.

IV. DEFINITIONS

Individual: Anyone who accesses or uses NKU's technology resources.

Technology Resources: All electronic devices, systems, networks, and software owned, operated, managed, or provided by NKU, including but not limited to computers, tablets, cell phones, servers, networks, internet access, email systems, data storage, electronic communications, and online services.

Traditional Works: Works including textbooks, monographs, papers, articles, musical compositions, replication packages, software, works of art and artistic imagination, unpublished manuscripts, dissertations, theses, popular nonfiction, novels, poems, syllabi, workbooks, laboratory manuals, and similar materials.

V. MONITORING AND PRIVACY

NKU may monitor, access, and disclose any information or data stored, transmitted, or received on its technology resources as necessary to ensure compliance with this policy, applicable laws, regulations, or other University policies; to protect the integrity, availability, and security of its technology resources; and/or for other legitimate University administrative purpose. Although NKU does not routinely access or disclose data created or stored by individuals on NKU's technology resources, NKU may do so when necessary for the purposes described in this policy. Access to user data must comply with relevant federal and state laws and typically will occur only after approval by the relevant area vice president and the General Counsel.

VI. ENFORCEMENT

By using NKU's technology resources, individuals agree to comply with this policy and all applicable laws and regulations. Failure to comply with this policy may result in disciplinary action and other consequences as outlined in this document.

Violations of this policy may result in disciplinary action in accordance with the University's policies, up to and including termination of employment, expulsion, academic penalties, or legal action, depending on the nature and severity of the violation. NKU may also report violations to appropriate authorities as required by law.

The University may also suspend, modify, restrict, or revoke an individual's access to NKU's technology resources, on a temporary or permanent basis, as necessary to address, mitigate, or investigate violations of this policy or other University policies or to protect the functionality and integrity of NKU's technology resources.

VII. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

NKU Data Governance website

U.S. Department of Education Family Educational Rights and Privacy Act (FERPA) guidelines

U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) regulations

U.S. Copyright laws

European Union General Data Protection Regulation (GDPR) laws

RELATED POLICIES

NKU Antivirus policy

NKU Data Governance & Security policy

NKU Information Security policy

NKU Records Management policy

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
Revision: Simplification/Clarification	February 8, 2024
Revision	April 12, 2019
Revision	April 23, 2018
Policy	September 1, 2008

ACCEPTABLE USE

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: 3/12/24.

☐ 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 Tammy Knochelmann *Date* 3/13/2024

Tammy Knochelmann