ACCEPTABLE USE

POLICY NUMBER: IT-ACCEPTUSE
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: CHIEF INFORMATION OFFICER
RESPONSIBLE OFFICE: OFFICE OF INFORMATION TECHNOLOGY
EFFECTIVE DATE: UPON PRESIDENTIAL APPROVAL – 4/12/19
NEXT REVIEW DATE: PRESIDENTIAL APPROVAL PLUS FOUR YEARS – 4/12/23
SUPERSEDES POLICY DATED: 4/23/2018
BOARD OF REGENTS REPORTING (CHECK ONE):
☐ PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM)
☒ PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

Overview

A trusted and effective information technology (IT) environment is vital to the mission and core values of Northern Kentucky University (NKU). NKU provides a wide variety of institutional electronic systems, computer services, networks, databases, and other resources. These are intended to support the educational, research, and work activities of members of the University's academic community and their external collaborators, to support the operations of the University, to provide access to services of the University and other publicly available information, and to ensure a safe and secure IT operating environment to all members of the University community.

The purpose of this policy is to define and promote the responsible use of information technology at NKU. Access to and usage of information technology resources necessitate certain expectations and responsibilities for all users.

Within NKU's IT environment, additional rules will apply to specific computers, computer systems, software applications, databases or networks or to college/departmental rules and activities. Departmental rules must be consistent with this policy, but may also impose additional, or more specific requirements or responsibilities on individuals. This policy will supersede any inconsistent provision of any departmental policy or rule. Computing resources covered by this policy include, without limitation:

- All University owned, operated, leased or contracted computers, networking, telephone, mobile devices, copiers, printers, media, and information resources, whether they are individually controlled, shared, standalone, or networked.
- All information and data maintained in any form and in any medium within the University's computer resources, including managed department and personal drives, or the Microsoft OneDrive service, provided through NKU.
- All University voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, and physical facilities, including all hardware, software, applications, databases, cellular devices, mobile devices, and storage media.

Three general principles underlie eligibility and acceptable-use policies for information technology:

- University information technology is for University faculty, students, and staff to use for core University purposes
- Some applications of University information technology may be unacceptable even if they serve core purposes
- Unauthorized access or use of University computing resources or data is strictly prohibited.

II. ENTITIES AFFECTED

Scope / Applicability
This policy applies to all persons using and/or attempting to access or use NKU computing resources regardless of whether these resources are accessed from NKU's campus or from remote locations. This includes but is not limited to University students, faculty and staff, authorized University guests, alumni, affiliates, agents of the administration, organizations accessing network services, and all individuals authorized for access or use privileges by the University.

III. RESPONSIBILITIES

Confidentiality
All individuals with access to confidential data are to utilize all appropriate and accepted precautions to maintain the accuracy, integrity, and confidentiality of the data and ensure that no unauthorized disclosures occur. Individuals are responsible to take appropriate action to insure the protection, confidentiality, and security of the University's information. Individual student records are subject to special protection as specified in the Family Educational Rights and Privacy Act (FERPA) of 1974 (https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn). Such data (e.g., Social Security numbers) must be handled with a high degree of security and confidentiality in compliance with policies, regulations, and laws, and must only be collected and stored when it is essential for approved business processes or to meet legal requirements. Violation of usage may be cause for dismissal from employment, disciplinary actions, and civil or criminal penalties.

- Refer to NKU's Information Security policy (https://inside.nku.edu/content/dam/policy/docs/Policies/InformationSecurity.pdf) for specific details to ensure confidentiality and integrity of University data.
- The University will access IT resources as necessary for system maintenance, including security measures. The Network Operations Center (NOC) and formally designated IT managers are authorized to monitor network traffic for malicious activity or suspicious patterns.
- The University's routine operation of IT resources may result in the creation of log files and other records about usage. This information is necessary to analyze trends, balance traffic, and perform other essential administrative tasks. IT may store incident-related data as required. IT may store aggregate data and usage logs for operational, compliance, and statistical purposes.
- The University may be compelled by a court of competent jurisdiction or a request for public records to disclose individuals' electronic records in response to various legal requirements, including subpoenas, court orders, search warrants, discovery requests in litigation, and requests for public records under the Kentucky Open Records Act or by request of the Office of General Counsel.

Individual Rights
NKU provides electronic resources to individuals to effectively perform their job duties. The University will not routinely monitor an individual's electronic data, software, or communication files, unless warranted by probable cause.

All individuals have the following rights:

- All individuals, including faculty, staff, students, authorized University guests, alumni, affiliates, agents of the administration, and community members are granted access to and permitted use of the University's electronic resources as related to specific purposes based on the individual's particular business needs or classification.
- Individuals have the authority to read, write, edit, or delete information in files or databases, as established by the designated roles and responsibilities of the individual, and according to NKU's

Records Management policy (https://inside.nku.edu/content/dam/policy/docs/Policies/Records%20Management.pdf).

- All individuals are provided with the University's on-campus network access, including electronic mail ("email") and internet access.
- Individuals have the right to receive training that will facilitate compliance with all responsibilities and restrictions set forth in this policy.

Individual Responsibilities

Data that is considered critical/sensitive or regulated must be securely housed within the IT data center or within approved safe electronic storage media. Highly sensitive data must be stored in compliance with NKU's Information Security policy (https://inside.nku.edu/content/dam/policy/docs/Policies/InformationSecurity.pdf). The University forbids the storage of highly sensitive data on any data storage device or media other than a centrally managed server ("employee"/"department" drives), or the Microsoft OneDrive service provided through NKU. Storing such data on hard drives (laptops, desktops, tablets, etc.) can subject the data to breach by viruses, malware, hacking, physical loss of device, etc.

If an individual is required to store highly sensitive data for a business need that is outside NKU managed networks, that individual must obtain permission from the Office of the CIO and the area Vice President. The written request for authorization must state the unique business need, the type of data that will be stored, the type of data storage device that will be used, and the mitigating controls that will be employed to protect the highly sensitive data. Each individual shall be responsible for the security and integrity of information stored on his or her personal desktop system, laptop, storage, and mobile devices. This includes:

- Maintaining current operating system, software, and firmware, as supported by the university
- Strictly following all data protection guidelines, including FERPA guidelines (https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn), HIPAA requirements (https://hhs.gov/hipaa/index.html) (and the European Union General Data Protection Regulation (GDPR) laws (https://gdpr-info.eu/)
- Installing, using, scanning, and regularly updating virus protection software (see NKU Anti-Virus policy https://inside.nku.edu/content/dam/policy/docs/Policies/Antivirus.pdf)
- All individuals accessing or storing university data on personally owned devices, such as mobile phones, tablets, and computers, are responsible to ensure security of the data through strong passwords and encryption to minimize risks of data leaks. Protected data may not be stored on personally owned devices unless effective security controls have been implemented to protect the data.
- Making regular backups of information and files
- Controlling and securing physical and network access to electronic resources and data
- Abiding by password protection practices, by choosing appropriate passwords, protecting the security of passwords, and changing passwords as needed
- Using only the access and privileges associated with his or her computer account(s) and utilizing those account(s) for the purposes for which they were authorized; however, incidental personal use of University technology resources is not prohibited by this policy. Incidental personal use is an accepted and appropriate benefit of being associated with NKU's rich technology environment. Appropriate incidental personal use of technology resources does not result in any measurable cost to the University and benefits the University by allowing personnel to avoid needless inconvenience. Incidental personal use must adhere to all applicable University policies. Under no circumstances may incidental personal use involve violations of the law or interfere with the fulfillment of an employee's University responsibilities.
- Respecting and honoring the rights of other individuals, with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright infringement, and use of electronic resources

- An individual suspecting that his or her access has been compromised is to report it to IT Security via abuse@nku.edu or the IT Help Desk and change passwords and access modes immediately.

Individual Restrictions

Individuals may NOT do the following:

- Provide access or passwords to any individual not authorized for such access
- Make use of accounts, passwords, privileges, or electronic resources to which they are not authorized
- Tamper with, modify, or alter restrictions or protection placed on their accounts, the University system, or network facilities
- Extend the network by introducing a hub, switch, router, wireless access point, or any other service or device that provides more than one device to the University network without consent and approval from IT network and security management
- Use the University's internet access or network in a malicious manner to alter, destroy, or improperly access any information available on the internet or on any network accessible device
- Share remote access authentication with other individuals
- Intentionally introduce, create or propagate computer viruses, worms, Trojan horses, or other malicious code to University electronic resources
- Use knowledge of security or access controls to damage computer and network systems, obtain extra electronic resources, or gain access to accounts, data, or information for which they are not authorized
- Eavesdrop or intercept transmissions, emails, or messages not intended for them
- Physically damage or vandalize electronic resources
- Attempt to degrade the performance of the system or to deprive authorized individuals of electronic resources or access to any University electronic resources
- Alter the source address of messages or otherwise forge email messages
- Send email chain letters or mass mailings for purposes other than official University business
- Use internal or external systems to relay mail between two non-University email systems
- Communicate or act on behalf of the University via any computing or internet form unless they have the authority to do so
- Install physical or virtual servers that have not been identified to and approved by the office of the CIO
- Install network game servers, either virtual or physical, unless authorized by the office of the CIO
- Install and/or download music, video, other copyright media, or software in violation of copyright laws
- Obtain access to NKU networks and computing devices if not an authorized individual
- Copy or distribute sensitive data regarding students, faculty, or staff without proper and approved safe storage devices, and only as required by the job duties

University Processes/Privacy

Individuals should be aware that centralized data, software, and communications files are regularly backed up to a storage area network (SAN) and stored for potential recovery. All activity on systems and networks may be monitored, logged, and reviewed by system administrators and/or governmental agencies, or discovered in legal proceedings or open records procedures. In addition, all documents created, stored, transmitted, or received on University computers and networks may be subject to monitoring by systems administrators.

The University will never disclose contents of communications to an outside entity unless formally instructed to do so by the Office of Legal Affairs and General Counsel and:

- When required by law. If necessary to comply with the applicable legal requirement, such disclosures may occur without notice to the individual or without the individual’s consent, as determined by the Office of Legal Affairs and General Counsel.

- In connection with a bona fide investigation by the University or an external legal authority into any violation of law or of any University policy, rule, or ordinance. When the investigational process requires the preservation of the contents of an individual's electronic records to prevent their destruction, the Office of Legal Affairs and General Counsel may authorize such an action.
- If appropriate University personnel determine that access to information in an employee's electronic account or file is essential to the operational effectiveness of a University unit or program and the employee is unavailable or refuses to provide access to the information.
- If the University receives an appropriately prepared and presented written request for access to information from the lawful representative of a deceased or incapacitated individual.

European Union (EU) General Data Protection Regulation (GDPR)

The EU GDPR provides broad privacy protections to students and faculty attending NKU from European countries. The GDPR also applies to NKU activities in the EU, for example, when a student attends a study abroad program in the EU or when a faculty member is temporarily assigned to work on behalf of NKU in the EU. When subject to the GDPR, NKU will comply with the regulation's core privacy principles.

Under the GDPR, NKU must have a lawful basis to process a data subject's personal data. Although there will be some instances where the processing of personal data will be pursuant to other lawful bases (e.g., processing necessary to protect the vital interests or safety of a data subject, processing related to legal action involving the university, etc.), the following lawful basis will apply to most NKU data processing activities:

- Processing for the purposes of the legitimate interests pursued by NKU or by a third party;
- Processing for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing for compliance with a legal obligation to which NKU is subject; and
- Processing pursuant to the consent of a data subject for one or more specific purposes.

GDPR Individual Rights of the Data Subject

Subject to all other applicable laws and regulations, including all laws of the United States and the Commonwealth of Kentucky, where legally applicable, certain individuals have the following rights under the GDPR:

- To access the personal data we maintain about you;
- To be provided with information about how we process your personal data;
- To correct or modify your personal data;
- To have your personal data deleted;
- To object to or restrict how we process your personal data;
- To request your personal data to be transferred to a third party; and
- To file a complaint.

Please be aware that under certain circumstances, the GDPR or other applicable laws may limit a data subject's exercise of the above rights. To exercise the above rights, individuals should contact http://dataquality.nku.edu/ (login required). Please note that exercising these rights is not a guarantee of a requested outcome.

University Rights

When compelled by court order, the University reserves the right to:

- Access, monitor, and disclose the contents of an individual's account(s)
- Access any University-owned technology resource and any non-University-owned technology resource, on University property, connected to University networks.
- Take this action:
    - To maintain the network's integrity

    - To maintain the rights of others authorized to access the network
    - To maintain the security of a computer or network system
    - To prevent misuse of University resources
    - To support the business of the University if impacted due to the sudden death, leave of absence, or incapacitation of an employee.
- Terminate access upon misuse.

In the absence of a court order, any such actions shall be taken only after the area Vice President appropriate to the circumstances makes a written determination that there is an urgent and compelling need to do so.

Non-Organizational Use
Users may not use electronic resources for:

- Compensated outside work, except as authorized by the Provost/Vice President for Academic Affairs pursuant to an approved grant or sponsorship agreement. Work completed in satisfaction of a faculty member's obligation to produce teaching materials, scholarly or creative activity, or service to the community is not considered "outside work," even if such work is compensated.
- The benefit of organizations not related to the University, except those authorized by a University dean, or the director of an administrative unit, for appropriate University-related service
- Personal gain or benefit
- Political or lobbying activities not approved by the Office of the Provost/Vice President for Academic Affairs
- Private business or commercial enterprise
- Illegal activities.

University electronic resources may not be used for commercial purposes, except as specifically permitted under other written policies of the University.

Any such commercial use must be properly related to University activities and provide for appropriate reimbursement to the University for taxes and other costs the University may incur by reason of the commercial use.

Enforcement: **Misuse of Electronic Resources**
In any case where Acceptable Use comes into question, University management reserves the right to determine what is appropriate and acceptable and what is not. Violations of University policies will result in one or more of the following actions:

- Individual will be notified that the misuse must cease and desist.
- Individual will be required to reimburse the University or pay for electronic resource(s).
- Individual will be denied access to the electronic resource(s), temporarily or permanently.
- The appropriate University disciplinary action will be initiated. Actions may include sanctions, up to and including termination of employment or expulsion, legal actions, etc.
- Law enforcement authorities may be contacted to initiate criminal prosecution.

Such penalties shall be levied through ordinary disciplinary procedures set forth in other official University personnel policy documents, such as the NKU Personnel Policies and Procedure Manual, the NKU Faculty Policies and Procedures (the "Faculty Handbook"), or the Chase College of Law Faculty Policies and Procedures (the "Chase Faculty Handbook").

All individuals are encouraged to report to abuse@nku.edu or the IT Help Desk any suspected violations of University computer policies, such as unauthorized access attempts.

Individuals are expected to cooperate with system administrators during investigations of system abuse. Failure to cooperate may be grounds for disciplinary action, expulsion, legal actions, fines, and other actions as

deemed necessary. If persuasive evidence exists of the misuse of electronic resources and that evidence points to a particular individual, the Office of the Chief Information Officer must be notified immediately.

The University retains final authority to define what constitutes proper use and may prohibit or discipline improper use the University deems inconsistent with this or other University policies, contracts, and standards.

Copyrights and Licenses

Software and media may not be copied, installed or used on university electronic resources except as permitted by law.

- Software installations must be communicated to and approved by IT Services. Proof of License, outlining the type and number of installations must be provided to the Office of Information Technology.
- Software, subject to licensing, must be properly licensed, and all license provisions (including installation, use, copying, number of simultaneous users, terms of the license, etc.) must be strictly adhered to.
- Creating or using unauthorized copies of software or media is a violation of this university policy. Such conduct may be in violation of the law and could subject the user to disciplinary action, fines, and/or imprisonment.
- All copyrighted information retrieved from electronic resources, or stored, transmitted or maintained with electronic resources, must be used in conformance with applicable copyright and other laws.
- Copied material, used legally, must be properly attributed in conformance with applicable legal and professional standards. See U.S. Copyright laws (http://www.copyright.gov/title17/).

Technical Maintenance and Administrative Rights

University System Administrators and Authorized IT Staff

All system administrators (those individuals charged with the daily administration of computer resources within a unit of the University) will preserve individuals' privileges and rights of privacy consistent with this and other applicable University policies. Access privileges will be used only to the extent required by the performance of job responsibilities. Administrators will take all reasonable steps necessary to preserve the availability and integrity of electronic resources, including:

- Reject or destroy email messages and email attachments that are suspected of containing malicious code, phishing, viruses, or worms.
- Eliminate sources of malware, viruses, phishing, or other forms of security threats, including shut down of ports, user names, passwords, and equipment, until it is safe to reconnect to network.
- Investigate and report suspected violations of University policies or viruses or other malfunctions.
- Ensure conformance with legal obligations as they pertain to the administration of electronic resources.

Physical Access Control

- Direct physical access to certain electronic resources such as servers, data networking devices, and telecommunications switches is restricted to authorized personnel only. If University personnel believe that an unauthorized person gained or attempted to gain access to a server or network equipment room, they must contact the Office of Information Technology and/or University Police immediately.
- Rooms containing critical electronic resources must be secured, and access to those rooms must be limited to authorized individuals only. All entrances to such rooms must be closed and locked at all times. Alarms, sensors, and other types of physical security systems must be utilized to further secure these facilities and to detect and report emergency conditions that might occur.
- Appropriate fire suppression systems must be in place. Authorized personnel may be granted access to server or network equipment rooms through the issuance of ID cards or keys or through the use of passwords or other access codes, and access is restricted to role-based authority.

Policy Amendments

- Northern Kentucky University reserves the right to change the policies, information, requirements, and procedures announced in this policy at any time. Changes required by University contractual commitments shall be effective and binding to individuals upon execution of any such contract by the University.
- An individual shall be deemed to have accepted and be bound by any change in University policies, information, requirements, or procedures announced in this policy at any time following announcement or publication of such change.

IV. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

NKU Data Governance website: http://inside.nku.edu/datagovernance.html/

U.S. Department of Education Family Educational Rights and Privacy Act (FERPA) guidelines: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn

U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) regulations: https://www.hhs.gov/hipaa/index.html

U.S. Copyright laws: http://www.copyright.gov/title17/

European Union General Data Protection Regulation (GDPR) laws: https://gdpr-info.edu /

RELATED POLICIES

NKU Anti-Virus policy: https://inside.nku.edu/content/dam/policy/docs/Policies/Antivirus.pdf

NKU Data Governance & Security policy: https://inside.nku.edu/content/dam/policy/docs/Policies/DataGovernance.pdf

NKU Information Security policy: https://inside.nku.edu/content/dam/policy/docs/Policies/InformationSecurity.pdf

NKU Records Management policy: https://inside.nku.edu/content/dam/policy/docs/Policies/Records%20Management.pdf

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
Revision	April 12, 2019
Revision	April 23, 2018
Policy	September 1, 2008

ACCEPTABLE USE

PRESIDENTIAL APPROVAL

PRESIDENT

Signature Ashvaidya Date 4/12/19

Ashish Vaidya

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: 5 / 8 / 19.

☐ 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.)

EXECUTIVE ASSISTANT TO THE PRESIDENT/SECRETARY TO THE BOARD OF REGENTS

Signature Wendy Peek Date 5/10/19

~~Benjamin Jager~~ Wendy Peek