ACCEPTABLE USE POLICY

POLICY NUMBER: RESERVED FOR FUTURE USE
RESPONSIBLE OFFICIAL TITLE: CHIEF INFORMATION OFFICER (CIO)
RESPONSIBLE OFFICE: INFORMATION TECHNOLOGY
EFFECTIVE DATE:9/1/2008

I. POLICY STATEMENT

1.0 Overview:

This policy applies to all persons using and/or attempting to access or use Northern Kentucky University computing resources. This includes but is not limited to University students, faculty and staff, authorized University guests, and all persons authorized for access
or use privileges by the University, hereafter referred to as ‘users’.

2.0 Scope:

Computing resources covered by this policy include, without limitation:

- All University owned, operated, leased or contracted computers, networking, telephone, mobile devices, copiers, 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

- 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.

Individual areas (e.g., departments, colleges) within the University may define supplemental policies or conditions of acceptable use for electronic resources under their control. These additional policies or conditions must be consistent with this policy but may provide additional detail, guidelines and/or restrictions. This policy will supersede any inconsistent provision of any departmental policy or condition.

Four 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

- Any use counter to this, or which interferes with core use by others, is unacceptable

- 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.

3.0 Policy: Confidentiality

All users 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 of 1974 (http://www.ed.gov/offices/OM/ferpa.html). Such data (e.g. SSN's) 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.

User Rights

The University provides electronic resources to users to effectively perform their job duties. The University will not routinely monitor an individual user's electronic data, software, or communication files, unless warranted by probable cause. All users have the following rights:

- All users are granted access to and permitted use of the University's Electronic resources as related to specific purposes based on the user's particular needs or classification

- Users have the authority to read, write, edit, ordelete information in files or databases, as established by the designated roles and responsibilities of the user, and according to the University Records Management policies

- All users are provided with the University's on-campus network access, including electronic mail ("email") and Internet access.

User Responsibilities

Data that is considered critical/sensitive or regulated/operational or copyrighted must be securely housed within the IT data center or within approved safe electronic storage media. Each user 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 the currency of operating system, software, and firmware, as supported by the University

- Strictly following all data protection guidelines, including FERPA guidelines

- Installing, using, scanning, and regularly updating virus protection software (see NKU Anti-Virus Policy)

- 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 on a regular basis

- 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

- 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

A user suspecting that his or her access has been compromised is to report it to IT Security via the IT Service Center and change passwords and access modes immediately.

User Restrictions Users may NOT do the following:

- Provide access or passwords to any user 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 through the Internet
- Share remote access authentication with other users or non-users
- 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 users 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
- Engage in activities that harass, degrade, intimidate, demean, slander, defame, interfere with, or threaten others
- Communicate or act on behalf of the University via any computing or internet form unless they have the authority to do so
- Install Servers that have not been identified to and approved by IT Services
- Install network game servers, unless authorized by the office of the CIO
- Install and/or download music, video, other copyright media or software per copyright laws
- Obtain access to NKU networks and computing devices if not an authorized user

- 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

Users should be aware that centralized data, software, and communications files are regularly copied to backup tapes 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 are considered University property, and may be subject to monitoring by systems administrators.

University Rights

The University reserves the right to:

- Access, monitor and disclose the contents of an individual user's account(s)
- Access, monitor and disclose the activity of an individual user's account(s)
- Access any University-owned technology resource and any non-University-owned technology resource, onUniversity property, connected to University networks.

This action may be taken:

- 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.

Any such action will be taken only after obtaining approval from the area vice president appropriate to the circumstances, or when compelled by court order, or when there is deemed to be an urgent and compelling need to do so. The university may terminate access upon misuse.

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. 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/).

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
- 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.

4.0 Enforcement:

Misuse of Electronic resources In any case where Acceptable Use comes into question, management of the University 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:

1.User will be notified that the misuse must cease and desist.
2.User will be required to reimburse the University or pay for Electronic resource(s).
3.User will be denied access to the Electronic resource(s), temporarily or permanently
4. The appropriate University disciplinary action will be initiated. Actions may include sanctions, up to and including, termination of employment or expulsion, legal actions, fines, etc.
5.Civil and/or legal action may be initiated.
6.Law enforcement authorities may be contacted to initiate criminal prosecution.

All users are encouraged to report to the IT Service Center any suspected violations of University computer policies, such as unauthorized access attempts. Users 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, IT management must be notified immediately. The University retains final authority to define what constitutes proper use and may prohibit or discipline use the University deems inconsistent with this or other University policies, contracts and standards.

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 users' 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, usernames, passwords, and equipment, until it is safe to reconnect to network
- Investigate and report suspected violations of University policies or virus or other malfunction
- 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's Department of Public Safety immediately. Rooms containing critical Electronic resources must be secured, and access to those rooms must be limited to authorized users 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.

5.0 Policy Amendments:

The 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 users upon execution of any such contract by the University. A user 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.

II. ENTITIES AFFECTED

Faculty, Staff, and Students

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
New Policy	09/01/2008
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	

Choose an item.	