Policy: PG-55

Subject: Technology Resource Acceptable Use

Approval Date: 02/26/99
Revision: 08/01/06

PURPOSE AND SCOPE

To establish acceptable guidelines for technology resource use by Morehead State University (MSU) faculty, staff, students, and sponsored guests; to establish and ensure adherence to best-practice technology security policies and procedures; and to ensure compliance with state, federal, and local laws and regulations.

ADMINISTRATION OF POLICY

The Division of Planning, Budgets, and Technology is responsible for the maintenance of this policy. Review by the President's cabinet and approval of the Morehead State University Board of Regents are required to make changes to this policy.

DEFINITIONS

Technology Users & Resources – Morehead State University faculty, staff, students, and sponsored guests using email, voice mail, pagers, cell phones, PDAs, network access, desktop computers, portable computers, wireless network access, printing resources, fax services, central computing resources, telephones, cable television, and all other technology resources not included herein owned by the University. This policy applies to technology users located at the MSU main campus, at regional campuses, and users accessing MSU owned resources via remote connections such as dialup, internet, or virtual private network (VPN) access.

Data Custodian – MSU employee assigned management responsibility for oversight of official University data that could include, but is not limited to, student records, financial records, personnel records, alumni records, inventory or facility information. For example, the Registrar is the data custodian for student academic records.

Authorized Access – permission granted to a technology user by a data custodian and/or appropriate supervisor to access technology resources for instructional, educational, research, or employment-related responsibilities.

Sponsored Guests – Individuals, associations, clubs, vendors, contractors, or other entities having a business, educational, fund-raising, or other affiliation with the University resulting in access to Morehead State University technology resources. Examples would be auxiliary service contract holders with office space on the MSU campus; retired faculty and staff; or federal, state, or local programs with offices located on MSU's campus.

University Need – includes University administration's determination that probable cause exists, that established security policies or procedures, University acceptable use and/or professional conduct policies and standards, or state, federal, or local laws and regulations have been violated, or are being violated. University Need may also exist to satisfy commitments or fulfill requirements of a business necessity.

Business Necessity – includes, but is not limited to, a civil suit, subpoena for discovery of e-documents or open records request.

ACCEPTABLE USE GUIDELINES

1. Administrative data base managers and data custodians have primary responsibility for insuring that access to data in the modules under their control and responsibility is restricted to those people with authorized access. Requests for official University information in any format should be routed through the appropriate data custodian with consultation of MSU legal counsel as necessary to assure compliance with privacy laws (FERPA & HIPAA) and/or state and federal open records laws.

2. Access and use of University resources is limited to faculty, staff, students, and sponsored guests. This includes access of the wireless network, email system, telephone system, desktop computers, and all other technology resources owned or controlled by the University regardless of method of access or physical location.

3. University technology resources shall be reserved for the official academic, business, or service functions of the University. Personal use of MSU technology resources for consulting, self-employment, or employment by other agencies is prohibited.

4. Compliance with state, federal, and local laws, rulings, and regulations must be maintained by all technology users at Morehead State University.

5. In order to ensure MSU faculty, staff, and students have access to safe and reliable technology resources, the integrity and operational stability of technology resources must be maintained.

PROHIBITED CONDUCT

The following list is not intended to be all-inclusive.

1. Copying University-owned or licensed software for personal or external use without prior written approval by the University and/or licensee.

2. Copying or modifying University-owned data files without authorized access.

3. Attempting to damage or disrupt operation of computing equipment, communications equipment, or communications lines.

4. Attempting to capture network traffic by any means including packet sniffing, or direct connection to the physical or wireless network infrastructure.

5. Using University technology resources for purposes other than those intended by granting access to technology resources to unauthorized persons, even if those persons are members of the University community.

6. Using University technology resources in self-employment activities unless authorized in accordance with University policy and procedures. Technology users may not use University technology resources to advertise for any commercial purposes.

7. Failing to protect an account, business process, and/or any form of sensitive data, including hard copy and electronic media, from unauthorized access. Sharing of a user ID and associated password or deliberately leaving a logged in account unattended is prohibited.

8. Installing unlicensed software on MSU computer equipment.

9. Using MSU technology resources to gain unauthorized access to other technology resources (regardless of ownership or location), to engage in illegal activity, or to violate MSU policies, regulations, or rules.

10. Sending email with a false return address or account ID, sending harassing email or inappropriate email messages, sending harassing or inappropriate text messages, making harassing or inappropriate phone calls, or otherwise creating a hostile work or academic environment via a technology resource. Sending chain mail or unauthorized mass mailings is prohibited.

11. Operating an unauthorized device or service including peer to peer hosts, radio frequency broadcast stations, streaming video servers, wireless access points, or any other technology resource that may conflict with or impair MSU's technology resources.

12. Except in conjunction with a bona fide research project or other academic undertaking, a user shall not knowingly use University-owned or leased computer equipment to access, download, print or store any information infrastructure files or services that depict nudity, sexual activity, sexual excitement or intimate sexual acts.

13. Failing to protect sensitive or mission critical data from loss or theft. It is the user's responsibility to take reasonable precautions to safeguard mission critical and/or sensitive data on their desktop or portable computer's hard drive.

VIOLATIONS: ADMINISTRATIVE AND/OR LEGAL ACTIONS

Violations of PG-55 Technical Resource Acceptable Use policy should be reported to the Director of Information Technology who shall coordinate administrative action in accordance with University policy. If state, local, or federal laws, rules, or regulations

are being or have been violated, the University Police Department and University legal counsel shall be notified at once.

With University Need, the University may monitor, inspect, transfer, archive or copy data, correspondence, documents, or other information both stored and in real time on any and all technology resources owned by Morehead State University. The University may disconnect from the campus network technology resources found to be in conflict with acceptable use guidelines. The University may take other appropriate action where illegal or improper usage is determined such as seizing technology equipment to facilitate forensic analysis by law enforcement and to preserve evidence in civil or criminal proceedings.

Morehead State University is the owner of all data/information stored on email, voice mail, centralized storage, and desktop computers. The data/information remains subject to all state and federal copyright laws and the University's intellectual property policy. Personal information stored on University owned systems is subject to inspection in the same manner as University information. With University Need, the University has the right to monitor, extend, limit, restrict, or deny access to its technology resources.

Access of a technology user's email or other electronic records shall only be done at the request of a Vice President, University legal counsel, or the President; or to comply with a court order presented by a recognized state, federal, or local law enforcement agency.

Those found to have violated state, local, or federal laws or University policies, rules, or regulations, may have their electronic access suspended and/or be suspended from employment with or without pay or be dismissed from employment, enrollment or association with the University in accordance with University policies. The University reserves the right to impose charges for the expenses incurred in such actions. All violations of state, federal, or local laws will be reported to law enforcement immediately.