11.2.2P
Volume 11, Information Management
Chapter 2, Technologies
Section 2, Code of Ethics for Computing and Communications
Approval Authority: Board of Regents
Responsible Executive: Vice President for Administration
Responsible Office(s): Information Technology
Effective: 10/8/94 **Issued:** 10/8/94
Last Revised: 01/25/13 **Next Review Date:** 01/25/18

Code of Ethics for Computing and Communications

Policy Statement

This policy defines the privileges and responsibilities of computer and communications users at Eastern Kentucky University. It is the expectation that all members of the University community adhere to every aspect of this Code. In addition to representing University regulations, many items are mandated by federal and state laws. Violations may result in severe penalties, up to and including expulsion or termination from the University.

Entities Affected by the Policy

All EKU Students, Faculty, and Staff

Policy Background

N/A

Policy Procedures

I. Using Information Technology Resources

A. University information technology resources are provided to faculty, staff, and students for the purposes of study, research, service and other work-related activities. Because resources are limited, all computer users must respect the priority of these purposes at all times.

1. To support these purposes, the University provides users with computers, peripherals, software, networks, and electronic communication services, including electronic mail, Internet access and electronic storage. Use of these devices and services may not interfere with the user's responsibilities to the University, or conflict with this Code. For example, computer users engaged in activities that are not directly related to work, study, research, or University related service must yield their computers to others who need them for those purposes.

2. University users must not share individual accounts or passwords with others (this includes co-workers, friends, and relatives); acquire accounts for which they are ineligible, or maintain accounts and privileges which are not relevant to their current role and assigned responsibilities.

3. The use of information technology resources must comply with U.S. and international copyright and licensing laws and their acceptable use provisions. Such use must also comply with laws defined by the Digital Millennium Copyright Act of 1998. The transmission or storage of all reproduced, distributed, altered, enhanced and/or manipulated copyrighted material must have prior written permission of the copyright holder.

B. The policies in this code apply to all hardware and software that make use of University resources, regardless of who owns the equipment or software licenses.

C. Use of University information technology resources to support a personal, profit-making activity is strictly forbidden.

D. The University generally does not monitor or restrict the content of material transmitted, stored, or posted on University information technology resources. However, the University reserves the right to monitor, limit or remove content or access to resources, when it has been determined by the appropriate University official that there is a violation or potential violation of applicable University regulations, contractual obligations, or state or federal laws. Individuals who use University information technology resources and email for any work-related or personal matters do not acquire an absolute right of privacy for data, documents and communications transmitted or stored on University information technology resources. Individuals are reminded that University information technology is University property and the individual has no expectation of privacy regarding any electronic communications, data or documents sent, received, or stored on University information technology.

II. Protecting Information Technology Resources and Institutional Data

A. Because information technology resources are limited and constitute a large investment by the University, all users must take proactive measures to protect these resources from malicious software, physical damage, and unauthorized access.

1. Individuals must comply with University protocol to minimize risks from viruses, phishing, and other technological threats.

2. Individuals must comply with all software licensing provisions, paying particular attention when installing software on multiple computers. No one should make copies of software for which permission to copy is not explicitly given. If the software does not allow users to copy it, then the software should not be copied.

3. Individuals must not use their access to computer systems to maliciously destroy or alter University accounts, files, software or hardware. Individuals must not attempt to obtain resources for which they are ineligible, or deprive others of resources.

4. Publishers may establish copyrights on digital material only in accordance with Eastern Kentucky University policies and U.S. laws.

B. Individuals with access to view or change sensitive institutional data must maintain the appropriate confidentiality, integrity, and security of that information, in accordance with University policies, as well as state and federal laws.

1. Individuals must not access information beyond that directly related to their current job assignments. Intentionally disclosing protected information to any unauthorized person is a violation of federal law (FERPA, HIPAA, etc.) and can subject the violators to University administrative, criminal and civil penalties.

2. Individuals with access to Personally Identifiable Information (PII) must take special care to use and transmit that data in an acceptable manner to prevent interception or misuse. For example: Email is not an acceptable method of transmitting PII.

III. Privacy of Information Technology Accounts

A. Account passwords are the primary means of ensuring privacy. Individuals must not share accounts or passwords.

B. When necessary for enforcing this Code, University policies or regulations, or public law, and when cause exists, authorized University personnel may access an individual's accounts and content to investigate possible violations. This may be done without securing permission.

C. University personnel who are authorized to access others' accounts to investigate possible violations must do so only under the direction of authorized personnel, and for no other purpose.

D. Electronic data and records will be released to appropriate authorities with authorization through a subpoena, warrant or other legal directive and may be subject to Open Records Requests.

IV. Electronic Communications

The use of information technology resources for unlawful purposes is prohibited. Examples of unlawful use include, but are not limited to: defrauding, threatening, abusing, defaming, harassing, intimidating or transmitting obscene messages or media. Using information technology is no different than similar conduct carried out in person, by telephone or by mail. Violations through electronic media will subject the individual to the same University sanctions.

In addition to the above, starting or extending email chain letters or spam is an example of an improper use of University resources.

Definitions

Information Technology Resources – Any technology, data, or service owned, housed, or contracted for use by the University, regardless of physical location.

PII – Personally Identifiable Information – Data which can be used alone, or with other information to uniquely identify, contact, or locate an individual. (e.g. social security number, date of birth, driver's license number, credit card number)

University-Eastern Kentucky University

Responsibilities

Associate Vice President for Information Technology:

Oversees University information technology resources.

Violations of the Policy

Violations of this policy could subject individual(s) to appropriate administrative and legal action; including any applicable provisions of faculty, staff, and student handbooks in coordination with other University units/departments e.g. Internal Audit, Office of University Counsel, or Equal Opportunity Office.

Interpreting Authority

Vice President for Administration

Statutory or Regulatory References

Digital Millennium Copyright Act of 1998 (DMCA)
Family Educational Rights and Privacy Act of 1974 (The Buckley Amendment) (FERPA)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Relevant Links

University Communications via University Email Accounts Policy 11.2.1P

Policy Adoption Review and Approval

Approved by EKU Board of Regents October 8, 1994
Revisions approved by EKU Board of Regents January 25, 2013