Eastern Kentucky University
Policy and Regulation Library

Administrative Regulation: 11.2.1ADR

Responsible Office(s): Information Technology

Effective: September 10, 2020

Next Review Date: September 2023

Administrative Regulation: 11.2.1ADR
Acceptable Use of Information Technology Resources

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 Policy. In addition to representing University policy, 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

All Users of Information Technology Resources

Procedures

I. Using Information Technology Resources

A. General Use of University Resources

1. University faculty, staff, and students must not share their 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.

2. The use of information technology resources must comply with U.S. and international copyright and licensing laws and their acceptable-use provision. 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.

3. The policies in this code apply to all hardware and software that make up University resources, regardless of who owns the equipment or software licenses. Because resources are limited, all users must respect the priority of the purposes of university academic and administrative business.

4. University resources and support services shall be used only to conduct University academic and administrative business. Use of University resources by employees to support a personal, profit-making activity is strictly forbidden.

5. In order to maintain the safety of all faculty, staff, students, and visitors, as well as to comply with state and federal law, the University reserves the right to monitor all content on University resources. In addition, the University may limit or remove content or access to resources to protect University resources, or when it has been determined by an appropriate University official that there is a violation or potential violation of applicable University policies, contractual obligations, or state or federal laws. Individuals who use University information technology resources, including electronic communications, for any work-related or personal matters do not acquire an absolute right of privacy for data, documents and communications sent, received, or stored on University resources.

B. University Computer Labs

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

To support these purposes, the University often provides users with computers, peripherals, software, networks, and electronic communication services, including email, Internet access, and electronic storage. Use of these devices and services shall not interfere with the user's responsibilities to the University, or conflict with this Policy. 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.

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 Information Security Policy to minimize risks from viruses, phishing, and other technological threats.

2. Individuals must comply with all software licensing provision, 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. Disclosing protected information to any unauthorized person is a violation of federal law and can subject the violators to University administrative, criminal and civil penalties. In order to mitigate the incidental harms to individuals, any disclosures of protected information should be immediately reported to the Department of Information Technology.

2. Individuals with access to Personally Identifiable Information (PII) must take special care to use and transmit the data in an acceptable manner to prevent interception or misuse.

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 University policies or regulations, or state or federal law, or when cause exists, authorized University personnel may access an individual’s accounts and content. This may be done without securing the individual’s permission.

C. University personnel who are permitted to access others' accounts for cause must do so only under the direction of authorized personnel.

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

A. An official EKU email address is established and assigned by Information Technology for each admitted student; each current full- and part-time faculty; and each full- and part-time staff in support of University operations and initiatives.

1. All university communications sent via email will be sent to this address.

2. All employees will use their official university email address to communicate with students.

3. All official university business conducted internally and with outside agencies via email will be done through the appropriate university email account. Any exceptions must be approved by the Office of University Counsel.

4. 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.

5. Distributing spam and/or phishing email is an example of an improper use of University resources.

B. Separation from the University

1. Students may access and use University technology resources until they graduate or become inactive. A student's status is determined using University records.

2. Employees may access and use University technology resources until their separation from the University.

3. A student or employee who has separated from the University is no longer authorized to utilize technology resources, even if their access has not been blocked by information technology services.

C. The University provides support for EKU email only and is not responsible for the handling of email by other service providers. Users should be aware that unless an exemption applies under state or federal law, all electronic communications may be considered public records and are subject to being disclosed.

Definitions

- **Active Student:** Individuals who have been admitted to the University, are eligible to register for courses at the University, or have registered for courses at the University within the past two years.

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

- **Personally Identifiable Information (PII)**: An individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
    - An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
    - A social security number;
    - A taxpayer identification number that incorporates a social security number;
    - A driver's license number;
    - state identification card number;
    - A passport number or other identification number issued by the United States government; or
    - Individually identifiable health information as defined in 45 C.F.R sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g (KRS 61.931 (6) (a-f))

- **Protected Information**: Any data that is subject to government statute or regulation (i.e., HIPAA, FERPA, etc.).
- **University**: Eastern Kentucky University (EKU).
- **Users**: Anyone who uses Information Technology Resources.

Responsibilities

- Chief Information Officer

    - Oversees University information technology resources
- University Counsel
    - Approves requests from external sponsors to use external sponsor's email account
- Users
    - Use IT Resources in compliance with this policy

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.

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)

Regulation Adoption Review and Approval

Regulation Issued

Date	Entity	Action
September 10, 2020	**Board of Regents**	**Adopted**