Kutztown University Policy ACA-069

Acceptable Use Policy

Purpose:

The purpose of this policy is to address the use of university issued/owned information technology resources.

Kutztown University provides numerous information technology resources for use by the university's students, faculty, and staff. The term Information technology resources includes, but is not limited to, all university computing equipment, personal data assistants, cellular phones, storage devices, and any electronic device issued by the university and intended for business purposes, as well as software, systems, and networks. These resources are provided to support the university's mission and institutional goals. The use of these systems is a privilege and all users are expected to act responsibly and to follow the university's policies and any applicable local, state, federal, and international laws and regulations (e.g., copyright, criminal use of a communication device, harassment, GDPR, etc.) related to the use of these resources.

Scope:

This policy applies to all users including faculty, staff, students, contractors and guest users of the Kutztown University computer network resources, equipment, or connecting resources. Use of the university's information technology resources signifies agreement to comply with this policy.

While the university recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that ideal, there should be no expectation of privacy of information stored on or sent through university-owned information technology, except as required by state or federal law. For example, the university may be required to provide information stored in its information technology resources to someone other than the user as a result of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. §67.101 et seq.). Information stored by the university may also be viewed by technical staff working to resolve technical issues.
This policy is subject to the terms and conditions of the various collective bargaining agreements that apply to faculty and staff.

Policy:

Acceptable Use of Information Technology Resources

A. Responsibilities of User of University Information Technology Resources:

1. Respect the intellectual property rights of authors, contributors, and publishers in all media;
2. Protect user identification, password, information, and system from unauthorized use;
3. Report lost or stolen devices, including devices that contain private or university information, to Information Technology Services (IT) within 24 hours of discovery of the loss;
4. Adhere to the terms of software licenses and other contracts. Persons loading software on any university computer must adhere to all licensing requirements for the software. Except where allowed by the university site licenses, copying software licensed for university use for personal use is a violation of this policy;
5. Adherence to all other applicable university policies and terms of any collective bargaining agreement;
6. To use the university information technology resources in a manner that complies with State and Federal law.
7. Use extreme caution when opening email attachments received from unknown senders, which may contain malware.

B. Prohibited Uses of University Information Technology Resources:

1. Providing false or misleading information to obtain a university computing account, or hiding or disguising one's identity to avoid responsibility for behavior in the use of information technologies;
2. Unauthorized use of another user's account;
3. Attempting to gain or gaining unauthorized access to university information technology resources, or to the files of another;
4. Performing any act(s) that impede the normal operation of or interfere with the proper functioning of university information technology resources, including, but not limited to, installation of hardware devices such as wireless routers, switches, and any other hardware connected to the network that impacts performance of university installed equipment;
5. Interfering with the security mechanisms or integrity of the university's information technology resources;
6. Use of the university information technology resources to transmit abusive, threatening, or harassing material, chain letters, spam, or other communications prohibited by state or federal law;
7. Copyright infringement, including illegal file sharing of video, audio, software or data;
8. Excessive use that overburdens the information technology resources to the exclusion of other users;
9. Excessive or prohibited personal use by employees;

    a. Incidental and occasional personal use (that is, non-job-related use) of information technology resources by employees is allowed as long as it does not interfere with the user's productivity and performance or that of

any other employee and as long as it does not adversely affect the efficient operation of the resources involved.

b. Personal use that violates the provisions of this or any other university policy is prohibited.

10. Use of the university information technology resources for personal profit, commercial reasons, non-university fundraising, political campaigns or any illegal purpose;
    a. The prohibition against using university information technology resources for personal profit does not apply to:
        i. Scholarly activities, including the writing of textbooks or preparation of other teaching material by faculty members; or
        ii. Other activities that relate to the faculty member's professional development.
11. Other activities as approved by the University President
12. Non-authorized solicitations on behalf of individuals, groups, or organizations are prohibited;
13. Intentionally or knowingly installing, executing, or providing to another, a program or file, on any of the university's information technology resources that could result in the damage to any file, system, or network. This includes, but is not limited to computer viruses, trojan horses, worms, spyware or other malicious program(s) or file(s);
14. Confidential information should not be stored on any non-University asset.

C. Enforcement:

A university employee or student who violates this policy risks a range of sanctions imposed by relevant university disciplinary processes, ranging from denial of access to any or all information technology resources up to and including termination (for an employee) or dismissal (for a student). He or she also risks referral for prosecution under applicable local, state or federal laws.

EFFECTIVE DATE:
December, 2009

ENDORSED BY:
President, November 5, 2009
University Senate, November 5, 2009
Administrative Council, November 20, 2009

LAST REVIEW:
January 28, 2010; August, 2010; August, 2011; August, 2012; August, 2013; August, 2014; August, 2015; August, 2016; August, 2017; August, 2018