KEAN

COMPUTER RELATED ACCEPTABLE USE POLICY

Preamble

Kean University ("Kean University," or "University") is committed to protecting and ensuring the ongoing availability and integrity of its data, and its information and/or computer systems through appropriate security measures and controls, and the promotion of a culture of security awareness. Effective security is a team effort involving the participation and support of all users who deal with data, information and/or computer systems. Therefore, it is the responsibility of all users to know these guidelines and to conduct their activities accordingly.

Overview

The purpose of these policies is to outline the acceptable use of information and/or computer systems and equipment at Kean University. Inappropriate use exposes Kean University to potential risks including, but not limited to, virus attacks, compromise of network systems, denial of services, and legal issues.

These policies protect Kean University, its students, faculty and staff, and information accessed, processed and stored, to ensure that Kean University can prevent, or reduce, undesired effects from internal and external threats, and to achieve continual improvement of Kean University's information security controls.

In the course of ensuring the ongoing protection and security of Kean University's information and/or computer systems and equipment, Kean University may monitor and record individuals' access to, and activities and use of, these systems. Anyone using any of the computer systems at Kean University expressly consents to such monitoring and recording and is advised that if such monitoring reveals possible evidence of criminal activity, Office of Information Technology ("IT") personnel may provide the evidence of such monitoring to law enforcement officials.

Roles and Responsibilities

The computer resources and facilities of Kean University are solely for the use of Kean University (registered) students, faculty and staff.

Users are expected to abide by the policies listed below. Those who do not abide by the policies should expect suspension of computer privileges and referral to the Office of Student Accountability, Standards & Education (for students) or the Office of Human Resources (for

employees). In some circumstances, offenders may also be subject to criminal prosecution under federal and state law and should expect IT to pursue such action.

Users must notify IT about actual or suspected violations of computer laws and policies, as well as about potential loopholes or vulnerabilities in the security of Kean University's computer system and networks. Users are expected to cooperate with IT in its operation of computer systems and networks as well as in its investigation of misuse or abuse.

Policies

The Kean University policies on Computer and Information Resources include but are not limited to the list below:

1. You must not use a computer ID that was not assigned to you by IT. You are responsible for all activity performed with your computer ID, and you must not permit others to use or perform any activity with your computer ID. You may not attempt to use or perform any activity with a computer ID belonging to another user, or try in any way to obtain a password for another's computer ID. You may not attempt to disguise the identity of the account or machine you are using.

2. You must not use IT's resources to gain unauthorized access to remote computers. If you abuse the networks to which the University belongs or the computers at other sites connected to those networks, the University will treat this matter as an abuse of your Kean University computing privileges.

3. You must not deliberately perform an act that will impact the operation of computer, terminals, peripherals or networks. This includes, but is not limited to, tampering with the components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines or interfering with the operation readiness of a computer.

4. You must not run or install on any university computer system or network, or give to another, a program that could result in the eventual damage to a file or computer system and/or the reproduction of itself. This is directed towards, but not limited to, the classes of programs known as computer viruses, Trojan horses and worms.

5. You must not attempt to circumvent data protection schemes or uncover security loopholes or vulnerabilities. Under no circumstances are users authorized to use computer systems to facilitate security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

6. Under no circumstances are users authorized to use computer systems to perform Port scanning or security scanning, or to use systems to circumvent user authentication or security of any host, network or account.

7. You must abide by the terms and conditions of all software licensing agreements, and under no circumstances are users authorized to use information and/or computer systems and equipment to violate copyrights, trade secrets, patents, or other intellectual property laws. Such conduct would include, but is not limited to, installing or distributing "pirated" software products.

8. You must not deliberately perform acts that are wasteful of computing resources. These acts include, but are not limited to, sending mass mailings or chain letters, obtaining unnecessary output, creating unnecessary multiple jobs or processes, or creating unnecessary network traffic.

9. The following types of information or software cannot be placed on any system on or off campus:
    - That which infringes upon the rights of another person.
    - That which is abusive, profane or sexually offensive to the average person.
    - That which consists of information which may injure someone else and/or lead to a lawsuit or criminal charges. Examples of these are: pirated software, destructive software, pornographic materials or libelous statements.
    - That which consists of any advertisements for commercial enterprises.

10. You must not harass others by sending annoying, threatening, libelous, or sexually, racially or religiously offensive messages. You must not send unsolicited messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e.g., e-mail spam). You are prohibited from enabling automatic forwarding of e-mail messages sent to your Kean University account to a third-party e-mail account.

11. You must not attempt to monitor another user's data communications, nor may you read, copy, change, or delete another user's file or software, without the permission of the owner.

12. You must not use any of the University's micro-computers, workstations or networks for other than a Kean University course, research project or departmental activity. These resources must not be used for personal gain unless in support of Kean University research or a departmental project.

13. You must not use a computer account for work not specifically authorized for that account. A University-funded account may not be used by its requestor for personal financial gain.

GUIDANCE GOVERNING ACCEPTABLE USE OF GENERATIVE AI TOOLS

Kean University is committed to harnessing the power of artificial intelligence (AI) to enhance learning experience, improve research capabilities, and streamline administrative processes. AI offers attractive opportunities to streamline work functions and increase efficiency. However, AI applications come with serious security, accuracy, and intellectual property risks. Therefore, it is essential that these technologies be used responsibly when integrated into university activities. This guidance outlines acceptable practices for utilizing AI tools while safeguarding institutional,

personal, and proprietary information. Additional guidance may be forthcoming as AI technology advances, however the following guidelines will help employees understand its acceptable use in the workplace while protecting the university's confidential or sensitive information, trade secrets, intellectual property, and brand. Training sessions, workshops, and resources will be available at IT Training to educate faculty and staff about best practices for AI implementation and ethical considerations.

NOTE: Expectations and guidelines for use of AI tools by students in courses is set forth in the Academic Integrity Policy. Students are required to adhere to the specific requirements outlined in each course syllabus.

Responsible Use Guidelines:

- Attribution – You should disclose when you have used an AI tool to help perform a task.
- Fact Check – AI tools are not a substitute for human judgment and creativity. AI tools may generate false or stale information and therefore their responses must be carefully verified by the employee.
- Restrictions on Employment Decisions – AI tools cannot be used by university employees to make or help make employment decisions, including but not limited to recruitment, hiring, retention, promotions, performance and discipline.
- Sanctioned AI Tools – AI tools that are sanctioned by the university for use by faculty and staff are identified on the IT Training webpage. As of June 23, 2025, the only sanctioned AI tool is **Microsoft Copilot Chat**, which is available through Microsoft Teams or the Office.com portal. Employees should use Copilot Chat for any AI-assisted tasks related to university work. Any other AI tools must be approved by the university and covered by contracts or published terms explicitly protecting university data in order for them to be authorized for use by faculty and staff. Confidential university information may only be used with university-sanctioned AI tools. ChatGPT or similar generative AI tools are not authorized for university business.
- Additional Restrictions on AI Tools not sanctioned by the university:
    - Do not upload or input personal information about any person.
    - Do not upload or input the name of Kean University or any department, division, center, program, school or college associated with Kean University.
    - Do not upload or input any confidential, proprietary, or sensitive information, such as passwords, ID numbers, student records subject to FERPA, protected health information, personnel

records, etc.
    - Do not use AI tools to record or transcribe meetings conducting university business unless the purpose for the recording or transcribing is made clear and all parties to the meeting expressly consent. Meetings involving personnel or other sensitive matters may not be recorded or transcribed.
- Do not use AI tools for activities that are illegal, fraudulent, or violate any federal or state laws or Kean University policy.
- Reporting Concerns or Abuse – Violations of these guidelines may result in disciplinary action, up to and including termination. Concerns about violations of these guidelines should be reported to your immediate supervisor.

POLICIES GOVERNING EXTERNAL NETWORKS

Kean University, from time to time, may provide computer data connectivity to external networks. This is especially important to support open research and education in and among U.S. research and instructional institutions, as well as support communication with foreign researchers and educators in connection with research or instruction. Traffic exiting the Kean network is governed by the policies of those networks in addition to the University's policies. Users connecting to external networks must abide by the policies of those networks.

Revisions Adopted:
6/23/25