KENNESAW STATE UNIVERSITY	Policy Title	Information Technology Acceptable Usage Policy
	Issue Date	February 1, 2007
	Effective Date	February 26, 2026
	Last Reviewed /Updated	October 9, 2025
	Responsible Office	Office of the Vice President of Information Technology and Chief Information Officer
	Contact Information	Office of the Vice President of Information Technology and Chief Information Officer, Office of Cybersecurity Phone: 470-578-6620 Email: ocs@kennesaw.edu

1. Policy Purpose Statement

An individual's use of computing resources in a university environment is not an absolute, personal right; rather it is a privilege conditional on the individual's compliance with federal and state laws, institutional policy, and generally acceptable use protocols. The Information Technology Acceptable Usage Policy defines what constitutes acceptable and unacceptable use of Kennesaw State University (KSU) computing facilities and resources. In using the computing resources of KSU, the user agrees to abide by all applicable University policies and procedures, and all applicable local, state, and federal laws. KSU reserves the right to review any accounts and files created on University resources. Per the University System of Georgia (USG) Appropriate Use Policy, individuals are held accountable for any misuse of their assigned network identification (NetID), computer system, and network access.

2. Background

The KSU Information Technology Acceptable Usage Policy was created to comply with the Georgia Computer System Protection Act and USG Appropriate Use Policy.

3. Scope (Who is Affected)

The KSU Information Technology Acceptable Usage Policy applies to all individuals utilizing University technology resources, including but not limited to students, faculty, staff, external contractors, retirees, and visitors.

4. Exclusions or Exceptions

Individuals may be exempted from this policy only upon written approval of the Office of the Vice President of Information Technology and Chief Information Officer.

5. Definitions and Acronyms

Definitions are available via the Information Technology Glossary in the KSU Policy Portal Glossary.

6. Policy

6.1 KSU accounts and technology resources are issued solely in support of the mission of the University. This includes activities that are considered educational but may not strictly relate to course content. Below is a list of criteria for the acceptable use of computing

resources and facilities at KSU.

6.1.1 No one shall use any University computer or network facility without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the University's computers or network facilities.

6.1.2 No one shall knowingly compromise, or attempt to compromise, the security of any University computer or network facility, nor willfully interfere with others' authorized computer usage, without prior written authorization from the CIO or designee.

6.1.3 No one shall use the University's communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer or network facility.

6.1.4 No one shall use the University's computing resources to harm the person, property, or reputation of another.

6.1.5 No one shall use the University's computing resources to violate the privacy and personal rights of another.

6.1.6 No one shall connect any device to a university network unless it meets generally accepted security standards including the latest operating system patch level and endpoint protection application if applicable.

6.1.7 All users shall share computing resources in accordance with policies set for the computers involved, giving priority to mission-related work and cooperating fully with the other users of the same equipment.

6.1.8 Users are required to store all institutional data in alignment with the Office of the Vice President of Information Technology and Chief Information Officer Document Management Matrix available at https://uits.kennesaw.edu/document-management/.

6.1.9 No one without specific authorization (see 4. Exclusions or Exceptions) shall use any University computer or network facility for non-University business.

6.1.10 KSU employees are responsible for maintaining accountability of technology assigned to them.

6.1.11 Users must keep passwords confidential. No one shall give any password for any University computer or network facility to any unauthorized person nor obtain any other person's password by any unauthorized means. The requesting and receiving of a user's credentials is prohibited.

6.1.12 No one except the designated system administrator in charge of a computer, or the system administrator's representative, is authorized to issue passwords for that computer.

6.1.13 No one shall misrepresent one's identity or relationship to the University when obtaining or using University computer or network privileges.

6.1.14 No one shall download, copy, install, transmit, or use any software or files in violation of applicable copyrights or license agreements, including but not limited to downloading and/or distribution of music, movies, software, or any other electronic media via the Internet.

6.1.15 Users are required to use their official KSU email account for service registrations.

6.1.16 No one may act as a sole vendor contact for third-party software or systems without approval from the Office of the Vice President of Information Technology and Chief Information Officer.

6.1.17 All users shall abide by all local, state, and federal laws when utilizing University computing resources.

6.1.18 Per the *USG Information Technology Handbook*, Section 5.2.1, USG Appropriate Usage Requirements, users are required to abide by a set of standards which

promotes responsible behavior and creates safeguards against the abuse of USG IT resources. As it is required to respect the privacy and personal rights of others, it is a violation to:

"Access or copy communications, data or files of other users without permission; and…Transmit, disseminate, sell, store or host material on USG resources that is unlawful, libelous, defamatory, obscene, pornographic, harassing, threatening, abusive or invasive of privacy rights.".

The Georgia Computer Systems Protection Act

The Georgia Computer Systems Protection Act was signed into law on July 1, 1991, and establishes certain acts involving computer fraud or abuse as crimes punishable by defined fines, imprisonment, or both. The act specifically defines common computer misuse scenarios such as computer theft, computer trespass, invasion of privacy, forgery, and password disclosure. The *Official Code of Georgia Annotated* (O.C.G.A.) § 16-9-93, states:

(a) Computer theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:
  (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;
  (2) Obtaining property by any deceitful means or artful practice; or
  (3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

(b) Computer Trespass. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:
  (1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;
  (2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or
  (3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

(c) Computer Invasion of Privacy. Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

(d) Computer Forgery. Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

(e) Computer Password Disclosure. Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and that results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500 shall be guilty of the crime of computer password disclosure.

6.2 Monitoring and Questions

6.2.1 Systems and accounts are monitored for inappropriate use.

6.2.2 Questions regarding proper usage should be addressed through the KSU Service Desk.

Faculty/Staff IT Service Desk	470-578-6999	https://service.kennesaw.edu
Student IT Service Desk	470-578-3555	https://service.kennesaw.edu

7. Associated Policies/Regulations

a. Georgia Computer System Protection Act (*Official Code of Georgia Annotated* (O.C.G.A.) § 16-9-93)
b. *USG Information Technology Handbook*, Section 5.1, USG Cybersecurity Program

8. Procedures Associated with this Policy

a. *Research Technology Standard*
b. *Bring Your Own Device Standard*

9. Forms Associated with this Policy

As required by policy, regulation, or procedure.

10. Violations

a. If a KSU employee or student witnesses any violation of policy, they should report it directly to the Office of the Vice President of Information Technology and Chief Information Officer via abuse@kennesaw.edu or (470) 578-6999. If any KSU employee or student witnesses a non-emergency criminal act, they should notify KSU Public Safety at (770) 423-6206. In the case of abuse, the rights of the users can be suspended.
b. Individuals using KSU computing resources are prohibited from using the system to commit a criminal act. This includes, but is not limited to, unauthorized access or attempt to access other systems; the implementation of any virus or malicious program; downloading and/or distributing music, movies, or any other electronic media in which legal copyright is not owned; or any use of the system to plan, commit, or exploit criminal activities.
c. Individuals found to be in violation of this policy may be subject to disciplinary action in accordance with the appropriate University handbook (https://handbooks.kennesaw.edu/). Punishments may include fines, suspension, termination, expulsion, and incarceration. Violations of local, state, and/or federal laws will be reported to the KSU Department of Public Safety.
d. UITS reserves the right to disable system accounts and user accounts if activity is inconsistent with applicable laws and university policies.

11. Review Schedule

The Office of Cybersecurity will review the Information Technology Acceptable Usage Policy annually.

12. Revision History

Origination Date: 02/01/2007
Revisions: 09/01/2024, 10/09/2025

*****For use by the KSU Institutional Policy Facilitator Only*****

At Kennesaw State University, institutional policies that have undergone the established shared governance review and feedback process are presented to the President and Provost for final approval. The signatures below indicate this institutional policy has been reviewed and approved by the President and Provost.

DocuSigned by:
Dr. Kathy Schwaig
11EA3F49C7FD4B9...

Dr. Kathy S. Schwaig
President
Kennesaw State University

DocuSigned by:
26412C41D0DE4E2...

Dr. Ivan Pulinkala
Provost and Executive Vice President for Academic Affairs
Kennesaw State University