Policy Title	Computer Usage Policy
Issue Date:	February 1, 2007
Effective Date:	November 21, 2016
Last Reviewed:	November 18,2016
Responsible Office:	Chief Information Officer
Contact Information:	University Information Technology Services/ Information Security Office Phone: (470) 578-6620 Email: iso@kennesaw.edu

1. 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 Computer Usage Policy defines what constitutes acceptable and unacceptable use of Kennesaw State University (KSU or the University) computing facilities and resources. In using the computing resources of KSU the user agrees to abide by all applicable University policies and procedures as well as 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 Kennesaw State University Computer Usage Policy was created to comply with the Georgia Computer System Protection Act and USG Appropriate Use Policy.

3. Scope

The KSU Computer 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 Chief Information Officer (CIO).

5. Definitions

Definitions are available via the Information Technology (IT) Glossary associated with this policy on the Policy at KSU website (policy.kennesaw.edu).

6. Policy

a. KSU access accounts 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.
   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.
   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.
   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.
   4) No one shall use the University's computing resources to harm the person, property, or reputation of another.
   5) No one shall use the University's computing resources to violate the privacy and personal rights of another.
   6) No one shall connect any computer to any of the University's networks unless it meets generally accepted security standards.[1] These include, but are not limited to, an antivirus application and the latest operating system patch level.
   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.
   8) No one without specific authorization (see 4. Exclusions or Exceptions) shall use any University computer or network facility for non-University business.

[1] See: http://csrc.nist.gov/publications/PubsSPs.html; http://benchmarks.cisecurity.org/

9) KSU employees are responsible for maintaining accountability of technology assigned to them.
10) 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 whatsoever. No one except the designated system administrator in charge of a computer, or his/her representative, is authorized to issue passwords for that computer.
11) No one shall misrepresent his or her identity or relationship to the University when obtaining or using University computer or network privileges.
12) No one without written authorization shall read, alter, or delete any other person's computer files or electronic mail. This rule applies regardless of whether the operating system of the computer permits these acts.
13) 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.
14) No one may act as a sole vendor contact, with regard to third- party software or systems without approval from the CIO.
15) All users shall abide by all local, state and federal laws when utilizing University computing resources.
16) Per the USG *Information Technology Handbook,* 5.1.4.2 "User Responsibilities", it is a violation to:
    i. upload, download, distribute, or possess pornography;
    ii. upload, download, distribute, or possess child pornography.
17) Per the USG *Information Technology Handbook*, 5.11.6 "Physical Security", devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 20 minutes.
18) Anyone who is unsure of whether something is allowed is encouraged to contact the KSU IT Help Desk for advice on whether a task is a legitimate use of an account.

Faculty/Staff IT Help Desk	470-578-6999	http://uits.kennesaw.edu/
Student IT Help Desk	470-578-3555	http://uits.kennesaw.edu/

Technology controls permit the logging of activities on University computer systems, and systems are regularly monitored for unauthorized use. Questions regarding proper usage should be addressed through the KSU IT Help Desk.

b. 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. Section 16-9-93 reads as follows (verbatim):

O.C.G.A. 16-9-93.

(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 which 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 $500.00 shall be guilty of the crime of computer password disclosure.

7. Associated Policies/Regulations

a. The Georgia Computer System Protection Act (OCGA § 16-9-93)
b. USG *Information Technology Handbook*, 5.1 Information Security Program

8. Procedures Associated with this Policy

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

9. Forms Associated with this Policy.

a. As required by information in Sections 7 and 8.

10. Violations

a. If a KSU employee or student witnesses any violation of this policy, they should report it directly to University Information Technology Services (UITS) 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 use

of 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.[2] Punishments may include fines, suspension, termination, expulsion, and possibly incarceration. Violations of local, state, and/or federal laws will be reported to the KSU Department of Public Safety.

11. Review Schedule

The Computer Usage Policy is reviewed annually by the Office of the CIO or his/her designee.

[2] See: http://kennesaw.edu/handbooks