Purpose:

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 state and federal laws, campus policy, and general acceptable use. The Computer Usage Policy seeks to define what constitutes acceptable and unacceptable use of Kennesaw State University computing facilities and resources. In using the computing resources of Kennesaw State University, the user agrees to abide by all applicable University Policies & Procedures as well as all applicable local, state, & federal laws. Kennesaw State University reserves the right to review any account and files created on university resources.

Definitions:

Definitions are available via the IT Glossary on the ITS Information Security Office website.

Scope:

The Kennesaw State University Computer Usage Policy applies to all individuals utilizing university technology resources including, but not limited to, students, faculty, staff, and external contractors.

Issue Date:

The Computer Usage Policy was issued on February 1, 2007.

Effective Date:

The Computer Usage Policy is effective as of January 1, 2011.

Policy:
Kennesaw State University access accounts are issued solely in support of the mission of the organization. This includes activities which are considered educational, but may not strictly relate to course content. Below is a list of guidelines for the acceptable use of computing resources and facilities at Kennesaw State University.

(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 connect any computer to any of the University's networks unless it meets generally accepted security standards. These include (but are not limited to) an antivirus application and the latest operating system patch level.

(5) All users shall share computing resources in accordance with policies set for the computers involved, giving priority to more important work and cooperating fully with the other users of the same equipment.

(6) No one, without specific authorization, shall use any University computer or network facility for non-University business.

(7) 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 system administrator in charge of a computer, or their representative, is authorized to issue passwords for that computer.

(8) No one shall misrepresent his or her identity or relationship to the University when obtaining or using University computer or network privileges.

(9) No one without specific 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.
(10) 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, or any other electronic media via the internet.

(11) No one may act as a sole vendor contact, in regards to 3rd party software or systems, without approval from the Vice President for Operations/CIO.

If you are not sure whether something is allowed, you are encouraged to contact the Kennesaw State University Help Desk to advise you on whether your task is a legitimate use of your account.

As with any other type of misconduct, incidents of computer misuse and abuse are dealt with in accordance with the judicial policy outlined in the University Catalog. Punishments may include fines, academic suspension, expulsion, and possibly incarcerations. Violations of local, state, and/or federal laws will be turned over to the Kennesaw State University Department of Public Safety.

Technology controls permit the logging of activities on University computer systems, and systems are regularly monitored for unauthorized use. If you have questions regarding proper usage, assistance should be sought through the Kennesaw State University Help Desk.

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 is excerpted below:

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.

Exceptions:
The Kennesaw State University Computer Usage Policy may only be exempted via approval from the Vice President for Information Technology.

Policy Violations:

If an employee or student witnesses any violation of policy they should report it directly to ITS via abuse@kennesaw.edu. If any employee or student witnesses a criminal act, they should notify KSU Public Safety. Information Technology
Services expects fair and responsible usage of KSU Computing resources. In the case of abuse, the rights of the users can be suspended.

Individuals using KSU Computing resources are prohibited from use of the system to commit a criminal act. This includes (but not limited to) unauthorized access or attempt to access other systems, the implementation of any virus or malicious program, downloading and/or distribution of 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.

Individuals in violation of this policy are subject to a range of sanctions including, but not limited to, the loss of computer or network access privileges, disciplinary action, dismissal from the University, and/or legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws.

**External Documents and Links:**

The Georgia Computer System Protection Act is available, in its entirety, at: [http://www.legis.state.ga.us/legis/2003_04/fulltext/sb103.htm](http://www.legis.state.ga.us/legis/2003_04/fulltext/sb103.htm)

**Review Schedule:**

The Computer Usage Policy will be reviewed annually by the Office of the Vice President for Operations/CIO or their designee.