KASKASKIA COLLEGE POLICY

Policy Name: Acceptable Use of Technology Resources
Subject Area: Business Services
Policy Number: #4.65
Approval Date: March 23, 2015

GENERAL

The Kaskaskia College Acceptable Use Policy promotes the efficient, ethical, and lawful use of the College's information technology resources. These resources are intended to support the educational, administrative, and public service missions of the institution. Access to these resources is granted subject to College policies and procedures, local, state, and federal laws.

SCOPE

This policy applies to all users of Kaskaskia College technology resources, whether affiliated with the College or not, and to all uses of those resources, whether at the main campus, education centers, or other locations, whether leased or owned by the College, in addition to personally owned devices connected by wire or wireless to the College network. Information technology resources consist of all College owned, leased, licensed computing hardware and software, email services, electronic devices, telecommunication systems, college network, and electronically stored data.

ACCEPTABLE USE

All users of Kaskaskia College information technology resources must:

- Comply with all Federal, Illinois, and other applicable laws; all generally applicable College rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include, but are not limited to, the laws of libel, privacy, copyright, trademark, obscenity, and pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking," and similar activities; the College's Student Handbook; the College's sexual harassment policy; and all applicable software licenses. Users who engage in electronic communications with persons in other

states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses. The use of College technology resources for viewing, receiving, sending or any other use of pornography, as defined by reasonable standards, is strictly prohibited and is subject to disciplinary action up to, and including discharge.

- Use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned to by the College. Ability to access technology resources does not, by itself, imply authorization to use such resources.
- Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Again, ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
- Respect the capacity of technology resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Although there is no set bandwidth, disc space, CPU time, or other limit to applicable uses of the College's technology resources, the College may, at its sole discretion, require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all relevant circumstances.
- Refrain from using those resources for personal commercial purposes or for personal financial or other gain. Personal use of College technology resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other College

responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures and the College has the sole discretion to determine whether personal use of technology resources is interfering with the performance of the user's job or other College responsibilities.

- Refrain from stating or implying that they speak on behalf of the College and from using College trademarks and logos without authorization to do so. Affiliation with the College does not, by itself, imply authorization to speak on behalf of the College. Authorization to use College trademarks and logos on College technology resources may be granted only by the Marketing Department, as appropriate.

ACCESS REQUIREMENTS

Access to information technology resources is granted by the Information Technology Department in the form of computer and network accounts to registered students, faculty, staff, and others as appropriate for such purposes as research, education, or College administration. Unique passwords are used to protect these accounts.

Accounts are assigned to individuals and are not to be shared. Each User is solely responsible for all functions performed from accounts assigned to them. It is a violation of this policy for any User to allow others (including other Users of the College network) to use or have access to his/her account. It is a violation to use another User's account, with or without that person's permission. Intentionally or negligently revealing one's password is prohibited. It is a violation to attempt to learn the password to another User's account, whether the attempt is successful or not.

The password used with an account, is the equivalent of an electronic signature. The use of a User ID and password authenticates an identity and gives on-line affirmations the force of a legal document.

Users are responsible for ensuring that they also comply with all Kaskaskia College information technology related policies. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

SECURITY AND PRIVACY

The College employs various measures to protect the security of its technology resources and of its users' accounts. In addition, users should engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users should also be aware that their use of College technology resources is not completely private. While the college does not routinely monitor individual usage of its technology resources, the normal operation and maintenance of the college's technology resources require the backup and caching of data and communications, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service.

The College may also specifically monitor the activity and accounts of individual users of College technology resources, including individual login sessions and communications, without notice, when the College, in its sole discretion, has determined that: (a) the user has voluntarily made them accessible to the public, as by posting to social networks or a web page; (b) it is necessary to do so to protect the integrity, security, or functionality of College or other technology resources or to protect the College from liability; (c) there is cause to believe that the user has violated, or is violating, this policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law. Any such individual monitoring, other than that specified in "(a)," required by law, or necessary to respond to emergency situations, must be authorized in advance by the appropriate Executive Level Administration.

The College, in its sole discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate College personnel or law enforcement agencies and may use those results in appropriate investigation proceedings and disciplinary actions.

REPORTING VIOLATIONS OF UNACCEPTABLE USE REGULATIONS

Violations of this Acceptable Use Policy should be reported immediately to the Information Technology Department or Vice President of Administrative Services. The College will make every effort to maintain confidentiality to the extent possible consistent with other obligations.

INVESTIGATIONS

In the event of any investigation, the College shall have the authority to examine all data or such other material that may aid in the investigation. The College reserves the right to access and review all information transmitted on the campus network. These include, but are not limited to: (a) investigating performance deviations and system problems (with reasonable cause); (b) determining if an individual is in violation of this policy; or (c) to ensure that the College is not subject to claims of institutional misconduct.

Authority to access user account information can only come from the Executive Level of Administration. External law enforcement agencies and Public Safety may request access to this information through valid subpoenas and other legally binding requests. All such requests must be approved by the Director of Legal Services, Risk Management, and Planned Giving. Information obtained in this manner can be admissible in legal proceedings.

DISCPLINARY ACTION

Users who violate this policy may be denied access to College technology resources and may be subject to other penalties and disciplinary action, both within and outside of the College. Violations will normally be handled through the College's disciplinary procedures applicable to the relevant user. The College may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of college or other technology resources or to protect the college from liability. The College may also refer suspected violations of applicable law to appropriate law enforcement agencies.

ACCEPTABLE USE EXAMPLES

The following scenarios are intended to provide examples of acceptable and unacceptable uses of information technology resources based on the Acceptable Use Policy. These examples are not comprehensive but are merely illustrations of some types of acceptable and unacceptable use.

- Acceptable Use:
  - While at your friend's house, you use their computer to connect to MyKC to check your email. After you have finished, you log off of your account, close the browser window, and make sure your email password was not saved on the computer.
  - While on vacation, you ask a staff person to check your email for you by forwarding your email to their account, removing the forwarding on your return.
  - You need to review some specific student data, so you call the IT Department and request access.
  - Your student worker does not have access to systems in order for her to do her job. You call IT and ask for her to have access.
  - As a student, you go to the Library to use the computer for study assignments and print out your homework.
  - You are running for political office. You use your personal email and home computer to promote your candidacy and refrain from sending the information to college-issued email addresses.
  - As a member of the Media Center, you store a video of a musical performance on the network.
  - Displaying a legally reproduced copy (with copyright notice) of a videotaped work in a classroom to a group of students and faculty as part of the instructional program.
- Unacceptable Use:
  - While your friend is using his/her computer, you give them your login and password to MyKC and have them open your email.
  - While on vacation, you ask another staff person to check your email by giving them your login and password.

- Another staff member is logging into Colleague and has access to student data that you do not. You ask for their login and password.
- When your student worker arrives at work you sign them into a computer using your own login and password.
- You wait until your classmates have left the computer lab, then you connect your USB drive to your computer and print out the invitations you made for your son's birthday party.
- While running for political office, you use your KC email account to send out email about your candidacy to people who live in your district, promoting yourself as a candidate.
- As a staff member, you download all the pictures from your iPhone and store them on the College's network so you can show everyone that stops by your desk.
- Playing a video in a classroom for entertainment purposes, or for its cultural or intellectual value unrelated to a teaching activity.