Acceptable Use

The intent of this policy is to define broad categories of use that are not acceptable, not to provide an exhaustive list of inappropriate or unacceptable uses. Based on the guidelines in this policy, HCTC officials may at any time make determinations that specific uses are or are not appropriate or acceptable. It is not acceptable to use the college's computer equipment or facilities:

- For any illegal purpose or act;
- To transmit harassing, indecent, obscene, discriminatory, or fraudulent materials or messages;
- To transmit or receive any materials in violation of either state or federal laws (e.g., copyright laws);
- To send fraudulent or forged email messages using the account of another person;
- To use the account or password assigned to another person to gain access to college equipment, college files, or the college network;
- To damage, destroy, interfere with, or disrupt the operation of, college owned and operated programs and equipment;
- For any commercial pursuits or activities;
- To access another user's files without permission;
- To access files by using false usernames, accounts, or passwords;
- To remove any college hardware, software, or data without permission;
- To copy or attempt to copy any software or data without authorization;
- To load, download or upload any software or files without authorization;
- To distribute unauthorized software;
- To modify system configurations or hardware without authorization;
- To disrupt or attempt to disrupt system operations;
- To participate in unauthorized and time-consuming game-playing;
- To harass another user or violate another user's rights;
- To access pornography or other offensive or inappropriate material;
- To use college computer systems and/or software for personal work;
- To use college computer systems, Internet access, and/or software for any illegal activity.

General Policies

- The use of food, drink, and tobacco products is not allowed in the computer labs.
- The user should be aware that HCTC computing resources, including software such as electronic mail, are not necessarily secure or private.
- Computers are for ACADEMIC use only. Game playing is not allowed in the computer labs. Any student using the computers for NON-ACADEMIC applications may be asked to log out.
- All users must have a user id and password to log into the campus computer system.
- Computer accounts and passwords are assigned to individual users and should not be shared with others.
- Students who do not LOG OFF a computer will risk losing their files or print allotments.
- Personal files left on will be deleted. Student work is to be saved to diskettes or USB key.
- Students are not to download files (e.g., chat clients or IRC programs, pictures, graphics) from the Internet to computer hard drives.
- Students are not to change any settings on the computers in the computer labs. This includes colors, screen savers, screen resolution, and icon arrangements.
- Computers are made available on a first-come, first-served basis. In the case of computers with special hardware and software, users not requiring these items can be asked to move to a different computer if someone needs to use the items.
- Be considerate of others by keeping noise and other disruptions to a minimum. Disruptive persons will be asked to leave.

The use of Hazard Community & Technical College computer technology is a privilege extended to all users, including faculty, staff, administrators, and students. Inappropriate or unacceptable use of this technology may result in loss of this privilege.

College agents may monitor information on the college computer network or on individual computers or computer systems. Complaints of possible inappropriate or unacceptable use will be investigated. Complaints regarding violations of acceptable use policy should be addressed to the Chief Information Officer. In investigating such complaints, the CIO will consult with appropriate college officials.

POLICY GOVERNING ACCESS TO AND USE OF KCTCS & HCTC COMPUTING RESOURCES

4.1 Five Dimensions:

Access to computing resources is granted to an individual by the Kentucky Community and Technical College System (KCTCS) solely for the grantee's own use. Derived from the values held by KCTCS, there are five dimensions of responsible use:

1. Privacy
2. Lawfulness
3. Integrity of Information and Information Technology
4. Equitable Distribution of Information Technology
5. Courtesy

It is unethical and a violation of the KCTCS Information and Information Technology Responsible Use policy for any person to violate these rights. All users, in turn, are expected to exercise common sense and decency (due regard for the rights of others) with respect to the public computing resources, thereby reflecting the spirit of community and intellectual inquiry at KCTCS. Access is a right that may be limited or revoked if an individual misuses the right or violates applicable KCTCS policies or state or federal laws.

4.2 Principles Governing Use of Computing Resources:

a. User access is granted to an individual and may not be transferred to or shared with another without explicit written authorization by the Vice President responsible for Technology Solutions, a designee, or the appropriate system administrator.
b. KCTCS expects individuals to obey laws related to information and information technology.
c. KCTCS expects individuals to ensure the integrity of the information and information technology.
d. KCTCS expects individuals to adhere to appropriate and efficient use of the information technology necessary to complete their assignments.
e. KCTCS expects individuals to use information technology in a manner consistent with maintaining optimal professional and respectful work and study environments.

4.3 Examples of Violations:

Violations of these principles or any attempt to violate these principles constitute misuse. Violations include, but are not limited to:

a. Viewing or distributing confidential or restricted information without authorization.
b. Sharing passwords or acquiring the password of another.
c. Failing to protect one’s own account from unauthorized use, e.g., leaving a publicly-accessible computer logged on but unattended.
d. Transferring confidential or restricted data without authorization to non-KCTCS devices, including home computers, removable memory devices, and personal digital devices.
e. Intentionally accessing, using, viewing, distributing, modifying, obscuring, or deleting of data, including information technology administrative data without proper authorization.
f. Creating or encouraging communications which may overload the communication network, including “email bombs,” “spam,” and “chain letters.”
g. Altering a communication of another individual without proper authorization.
h. Installing on KCTCS information technology software which damages information or restricts the utility of the information technology, e.g., “computer virus.”
i. Altering existing information technology without proper authorization.

4.4 Responses to Violations:

Violation of this policy will result in action by the appropriate KCTCS office or agency. Violations of KRS 434.840 (Kentucky statutes dealing with unlawful access or use of a computer) may be referred to the Commonwealth Attorney or the police for investigation and/or prosecution. Similarly, violations of 18 U.S.C. Sec. 1030 (Federal laws dealing with unlawful access or use of a computer) may be referred to the Federal Bureau of Investigation.

4.5 KCTCS Sanctions:

KCTCS sanctions are imposed by the appropriate KCTCS authority and may include, but are not limited to, limitation or revocation of access rights and/or reimbursement to KCTCS for the computing and personnel charges incurred in detecting and proving the violation of these rules, as well as from the violation itself. Reimbursement may include compensation for staff work time related to the violation and for archiving information related to the incident. The usual rights and privileges of appeal apply.

4.6 Investigating and Review of Charges:

When the Vice President responsible for Technology Solutions, a designee, or the appropriate college administrator has reason to believe that a violation may have occurred, the Vice President may initiate an investigation and/or suspend computing privileges for the individual(s) involved, pending further investigation. If significant KCTCS sanctions are imposed, such action, together with an explanation of the causal events, shall be reported by the Vice President to the Chancellor and the chief executive officer or designee.