4.2.5 Information and Information Technology Responsible Use Policy

KCTCS expects all individuals to responsibly use information and the information technology employed to collect, process, store, and disseminate it.

Along with its reputation, students and employees, funds, and facilities, information and information technology are among the most valuable assets of KCTCS.

4.2.5.1 Scope

This policy applies to the entire academic community of students, employees (both faculty and staff), affiliates, and authorized guests. Every individual using KCTCS information technology is responsible for reading this policy and completing and adhering to the compliance agreement.

This policy is compatible with other KCTCS policies and procedures, particularly policies related to ensuring a harassment-free, discrimination-free, respectful, and professional education/work environment.

Information is data about people, objects, and events, as well as derivations of these data.

Whether in transit or stored in a shared server, workstation, laptop, personal digital device, file cabinet, or wastebasket, information shall be subject to appropriate and consistent protection. Information may be text, sounds, and images in electronic form, as well as on paper and other tangible media.

Information created using KCTCS information technology is an asset of KCTCS. The information includes confidential and restricted information as well as public information.

Information technology is software, hardware, and the communication networks to which they may be connected. The hardware includes computers, personal digital devices, cell phones, radios, and televisions. The information technology includes data, audio, and video systems, including telephone and television.

KCTCS information technology includes all hardware, software, and communication networks that KCTCS owns, leases, or has been assigned control. It also includes non-KCTCS hardware and software while it is connected to the KCTCS communication network or to other KCTCS information technology.

4.2.5.2 Dimensions of Responsible Use of Information and Information Technology

Derived from the values held by KCTCS, there are five dimensions of responsible use: Privacy, Lawfulness, Integrity of Information and Information Technology, Equitable Distribution of Information Technology, and Courtesy.

Privacy
KCTCS expects individuals to ensure the privacy of the personal information about others. Disrespecting the right to privacy is in many cases illegal, and hardship is likely for the individual whose privacy is compromised.

While KCTCS endeavors to secure personal files, the first priority is the security of KCTCS information. Additionally, KCTCS has the right to view personal files and to remove personal files found in violation of this policy.

Access to KCTCS information and information technology is granted to an individual and may not be transferred to or shared with another without explicit written authorization by the KCTCS Vice President primarily responsible for Technology Solutions or designee.

Lawfulness
KCTCS expects individuals to obey laws related to information and information technology.

Integrity of Information and Information Technology
KCTCS expects individuals to ensure the integrity of the information and information technology.

The quality of the information and the condition, reliability, and performance of the information technology is critical to KCTCS.

Equitable Distribution of Information Technology
KCTCS expects individuals to adhere to appropriate and efficient use of the information technology necessary to complete their assignments.

Information technology use may be limited to only those activities needed for students to complete their class work and employees to complete their assigned duties.

Information technology must be shared among individuals in an equitable manner. Individuals must avoid any behavior that interferes with the equitable distribution of information technology.

Courtesy
KCTCS expects individuals to use information technology in a manner consistent with maintaining optimal professional and respectful work and study environments.

4.2.5.3 Confidential and Restricted Information

A specific focus of this policy is placed on confidential and restricted information, since KCTCS values the privacy of the individual. Within the central repositories, each data item or dataset shall be categorized to ensure that sensitive information is limited to those who have a business reason to use it.

KCTCS expects individuals to safeguard confidential and restricted information from irresponsible use. Confidential information, the highest level of sensitivity, is defined by

substantial damage to or liability by KCTCS if treated irresponsibly. Restricted information is defined by the need for special safeguards beyond that taken for public information. While public information, the lowest level of sensitivity, requires no safeguards, its accuracy is very important. Specific rules, guidelines, and definitions have been developed to safeguard the information entrusted to KCTCS.

All forms of recorded information: written, oral, and visual, regardless of the media, including paper and electronic, shall be safeguarded. The external distribution of confidential and restricted information regardless of the media, including electronic and paper, shall be limited. Particular care shall be taken with information in electronic form or derived from electronic form since the quantity of information distributed is likely to be large.

Information, wherever it is created, processed, transmitted, stored, or scheduled for destruction, shall be protected from inappropriate access, modification, disclosure, and destruction. As a result, information must be protected according to its sensitivity, criticality, and value, regardless of the media in which it is stored, the manual or electronic system that processes it, or the method by which it is distributed.

Confidential and restricted information shall be encrypted during transmission into non-KCTCS communications networks.

4.2.5.4 Communication Network and its Services

A special focus is placed on the KCTCS communication network and its services, since confidential and restricted information, as well as critical information technology, is accessible from connected devices.

KCTCS expects all individuals, particularly information technology staff, to safeguard the networked services and the communication network from irresponsible use. Specific rules and guidelines have been developed to safeguard the information entrusted to KCTCS and ensure the equitable distribution of the communication network and its services, including servers, cabling, access points, and related network devices, among the academic community of students, employees (both faculty and staff), affiliates, and authorized guests.

4.2.5.5 Information and Information Technology Responsible Use Compliance Agreement

Before being granted access confidential or restricted information every individual must show photo identification, e.g., driver license, and then complete and sign the compliance agreement in which he/she agrees to comply with the *Information and Information Technology Responsible Use Policy*.

The compliance agreement shall be available for electronic, as well as handwritten, signature. Other accommodations shall be made pursuant to the Americans with Disabilities Act of 1990 (Public Law 101-336).

4.2.5.6 Roles and Responsibilities for Ensuring Responsible Use of Information and Information Technology

The KCTCS President has ultimate responsibility for the information, including that information intended to reside primarily at the System Office, and for the information technology on which it is stored or processed.

The KCTCS President shall:

- Approve revisions to this policy.
- Annually review a summary prepared by the KCTCS Vice President primarily responsible for Technology Solutions of the system- and college-level security reports, and, if necessary, direct the revision of this policy and associated rules, guidelines, and definitions.
- Provide opportunities for the entire academic community to identify and implement best practices in responsible use of information and information technology and for the information technology administrators to refine their skills in safeguarding information and information technology.

The KCTCS President may:

- Delegate to the KCTCS Vice President primarily responsible for Technology Solutions oversight of the information which resides at the System Office and all information technology, including the information technology which resides at the colleges.
- Delegate to each college president/chief executive officer oversight of information which resides at the college and supervision of information technology which resides at the college.

The KCTCS Vice President primarily responsible for Technology Solutions shall ensure that the information within central repositories is secure and available. In addition, the KCTCS Vice President shall ensure that the information technology shared across KCTCS, including the communication network, is secure, available, and equitably used. The KCTCS Vice President is empowered to grant exceptions to this policy in consultation with the KCTCS President.

The KCTCS Vice President primarily responsible for Technology Solutions shall:

- Review and forward to the KCTCS President modifications to this policy.
- Communicate this policy regularly to the academic community.
- Interpret this policy with advice of the KCTCS President and Cabinet officers.
- Investigate any allegation of irresponsible use, determine whether the allegation is correct, and, if so, refer the incident to the KCTCS Vice President primarily responsible for Human Resources if an employee is involved or to the KCTCS Chancellor if a student is involved. The Vice President primarily responsible for Technology Solutions shall report the incident and its disposition to the KCTCS President.
- Appoint a system-level Information Security Officer within the KCTCS Office of Technology Solutions to serve as the custodian of all information owned by KCTCS which is stored centrally, particularly the central database system.

The KCTCS Chancellor shall:

- Oversee the content within the central repositories with respect to student records and assign a unit designee with direct operational-level responsibility for information management for these records who will be responsible for data access and policy implementation issues.
- Foster the integrity of information related to student records.
- Oversee any disciplinary action taken related to irresponsible use of information and information technology by students.
- Report students suspended, expelled, or placed on restricted access to the system-level Information Security Officer in order for access to information and information technology to be changed.

The KCTCS Vice President primarily responsible for Human Resources shall:

- Oversee the content within central repositories with respect to Human Resources and assign a unit designee with direct operational-level responsibility for information management for these records who will be responsible for data access and policy implementation issues.
- Foster the integrity of information related to Human Resources.
- Oversee any disciplinary action taken related to irresponsible use of information or information technology by employees, affiliates, and authorized guests.
- Report terminations to the system-level Information Security Officer in order for access to information and information technology to be changed.

The KCTCS Vice President primarily responsible for Finance shall:

- Oversee the content within central repositories with respect to Financial records and assign a unit designee with direct operational-level responsibility for information management for these records who will be responsible for data access and policy implementation issues.
- Foster the integrity of information related to Finance.

The KCTCS Vice President primarily responsible for Institutional Advancement shall:

- Oversee the content within the central repositories with respect to Advancement records and assign a unit designee with direct operational-level responsibility for information management for these records who will be responsible for data access and policy implementation issues.
- Foster the integrity of information related to Advancement.

KCTCS legal services shall monitor the legislation for potential impact on this policy and its execution, as well as advise the KCTCS leadership on the legality of actions related to irresponsible use, including its investigation.

The system-level Information Security Officer shall be responsible for the security of information.

The system-level Information Security Officer shall:

- Draft and forward to the KCTCS Vice President primarily responsible for Technology Solutions modifications to this policy.
- Refer allegations of irresponsible use to the KCTCS Vice President primarily responsible for Technology Solutions for investigation.
- Serve as the primary contact for issues related to confidential and restricted information and information technology.
- Establish rules, guidelines, and definitions for responsible use.
- Manage the creation, change, and removal of privileges to access System Office information and information technology either directly or by delegation.
- Ensure that appropriate security controls are enabled and being followed in coordination with the each of the unit designees of central repositories, including:
    - Classifying data items within each of the central repositories as "Confidential or Restricted", or "Public" and ensuring security is maintained at an appropriate level based on the classification.
    - Administer policies and procedures for granting and maintaining access privileges for systems containing confidential or restricted information.
- After each security incident the security officer will conduct a review of the measures put in place to prevent further incidents.
- At least annually, review the status of the KCTCS network security and provide a report to the KCTCS Vice President primarily responsible for Technology Solutions.

The college presidents/chief executive officers shall oversee information intended to reside primarily at the college and supervise the information technology located at their college.

The college president/chief executive officer shall:

- Communicate this policy regularly to the academic community of the college.
- Identify problem areas to the KCTCS Vice President primarily responsible for Technology Solutions, and, if necessary, propose changes to policy, rules, guidelines, and definitions to improve security or reduce irresponsible use, as well as to the system-level Information Security Officer.
- Appoint a college-level Information Security Officer to serve as the custodian of all information stored exclusively at the college.

The college-level Information Security Officer shall oversee the security of information residing primarily at the college.

The college-level Information Security Officer shall:

- Refer allegations of irresponsible use to the KCTCS Vice President primarily responsible for Technology Solutions for investigation, as well as the college president/chief executive officer.
- Manage the creation, change, and removal of privileges to access college information and information technology either directly or by delegation.
- Ensure that appropriate security controls are enabled and being followed in coordination with information technology administrators responsible for security administration at the college, including:

  - Classifying data stored locally at the college as "Confidential or Restricted", or "Public" and ensuring security is maintained at an appropriate level based on the classification.
  - Administer policies and procedures for granting and maintaining access privileges for systems containing confidential or restricted information
- After each security incident the security officer will conduct a review of the measures put in place to prevent further incidents.

The information technology administrators, including those with faculty rank, have additional responsibilities. In order to safeguard all information and information technology, they not only have access to nearly all information in electronic form and all information technology but also control the access of others.

4.2.5.7 Annual Review and Test of Responsible Use of Information and Information Technology

KCTCS employees will be required annually to review the requirements for responsible use of information and information technology, take and pass a test concerning those requirements, and record the results of the test with Human Resources.

4.2.5.8 Non-compliance Regarding Responsible Use of Information and Information Technology

KCTCS students, employees, affiliates, and authorized guests shall comply with related laws and KCTCS policy. Violations shall not be permitted and shall be addressed appropriately by KCTCS and law enforcement agencies.

4.2.5.8.1 Examples of Non-compliance Regarding Responsible Use of Information and Information Technology

Violations of this policy or any attempt to violate this policy constitute irresponsible use. Violations include, but are not limited to:

Privacy

- Viewing or distributing confidential or restricted information without authorization.
- Sharing passwords or acquiring the password of another.
- Failing to protect one's own account from unauthorized use, e.g., leaving a publicly-accessible computer logged on but unattended.
- Transferring confidential or restricted data without authorization to non-KCTCS devices, including home computers, removable memory devices, and personal digital devices.
- Storing confidential or restricted information on a portable device (such as a laptop, personal digital assistant (PDA), cell phone, or an external storage device) that is subject to loss or theft without authorization and without carrying out proper safeguards.

Lawfulness

- Copying, moving, or capturing licensed software for use on a system for which the software is not licensed or for use by an individual for which the software is not authorized.
- Communicating text or images using KCTCS information technology that are likely to be considered by KCTCS employees or students to contribute to an offensive or discriminatory work or academic environment.
- Representing the institution using information or information technology without proper authorization.
- Selling or bartering information or access to information technology.
- Disabling security on information technology without proper authorization.
- Concealing one's own identity in bad faith, i.e., with the intent to deceive.

Integrity of Information and Information Technology

- Intentionally accessing, using, viewing, distributing, modifying, obscuring, or deleting of data, including information technology administrative data without proper authorization.
- Installing on KCTCS information technology software which damages information or restricts the utility of the information technology, e.g., "computer virus".
- Altering a communication of another individual without proper authorization.
- Altering existing information technology without proper authorization.
- Failing to provide the key to encrypted information as this may interfere with investigations of irresponsible use.

Equitable Distribution of Information Technology

- Intentionally wasting information technology resources, including central processing unit time, storage, network capacity, printing resources, and related supplies.
- Denying access by another individual to information or information technology to which they are authorized.
- Using information technology for non-KCTCS-related purposes on a routine or extended basis.
- Creating or encouraging communications which may overload the communication network, including "email bombs", "spam", and "chain letters".

Courtesy

- Using or allowing use of information technology to access materials likely to be considered pornographic by institution leadership.
- Using information technology to advance a personal opinion (except where allowed by free-speech, in which case it must be clearly noted that the opinion does not necessarily reflect the opinion of KCTCS or where authorized in writing by the KCTCS Vice President primarily responsible for Institutional Advancement and Communication).
- Making allegations of irresponsible acts by others in bad faith, i.e., with an intent to deceive.

4.2.5.8.2 Potential Implications of Non-compliance Regarding Use of Information and Information Technology

For a student found to have made irresponsible use of information or information technology, the consequences shall be appropriate disciplinary action up to, and including, but not limited to, expulsion.

For an employee found to have made irresponsible use of information or information technology, the consequences shall be disciplinary action as appropriate, up to and including, but not limited to, termination.

In additional, KCTCS may require the individual to reimburse KCTCS for the computing and personnel charges incurred in the investigation of violation of the rules, including compensation of staff hours and costs for external services provided.

As appropriate, an employee may receive additional training related to the use of information or information technology, be reassigned to another position or other duties in which the employee will not be responsible for using the particular information or information technology, and/or have all or part of their access to information or information technology changed or revoked.

Violations of KRS Chapter 434.840 (*Unlawful access to 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 (*Computer Fraud and Abuse Act*) may be referred to the Federal Bureau of Investigation.

9-5-00	9-18-00; 6-21-06; 5-10-07; 5-20-08	9-18-00; 6-21-06; 5-10-07; 5-20-08
Approval Date	Date(s) of Last Review	Date(s) of Last Revision *(Include all dates in chronological order)*

(SIGNED)	5-20-08	(SIGNED)	5-20-08
Recommended by	Date	President, KCTCS	Date