4.2.5 Information and Information Technology Responsible Use Policy

This policy applies to the entire KCTCS community of students, employees (both faculty and staff), affiliates, and authorized guests. **KCTCS requires all individuals to responsibly use information and the information technology employed to collect, process, store, and disseminate it. Acceptance of this policy shall be acknowledged before being allowed access to KCTCS information technology.**

This policy complies 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. Information may be text, sounds, and images in electronic form, as well as on paper and other tangible media. Information shall be subject to appropriate and consistent protection, whether in transit, stored in a shared server, cloud storage, workstation, laptop, personal digital device, file cabinet, or wastebasket, copier, fax, database, or other possible locations.

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 (IT) is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data. 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.

4.2.5.1 Categories of Responsible Use of Information and Information Technology

Derived from the values held by KCTCS, there are five categories of responsible use: Privacy, Lawfulness, Integrity of Information and Information Technology, Improper Use of Information and Information Technology, and Courtesy.

Privacy
KCTCS requires faculty, staff and students to ensure the privacy of personal information. Violating or disregarding an individual's right to privacy is a violation of this policy.

KCTCS technology and information technology user account information, including but not limited to user passwords, may not be transferred to or shared with another without explicit written authorization by the KCTCS Legal Services in consultation with KCTCS Vice-President responsible for Technology Solutions.

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

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

Improper Use of Information and Information Technology Resources
KCTCS requires individuals to utilize information and information technology resources for business and educational related purposes only.

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

4.2.5.2 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 legitimate educational or KCTCS business-related purpose to use it.

KCTCS requires individuals to safeguard confidential and restricted information from irresponsible use. Confidential information, the highest level of sensitivity, is defined as information that could cause substantial damage to or liability for KCTCS if treated irresponsibly. Restricted information is defined by the need for special safeguards beyond that taken for public information. Public information, the lowest level of sensitivity, may be released according to rules, guidelines, and definitions developed to safeguard the information entrusted to KCTCS. All information in this policy includes the secure transmission and disposal of information or information technology.

All forms of recorded information and access to that 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. Safeguarded precautions shall be utilized when providing information in electronic form or other media.

4.2.5.3 Information and Information Technology Responsible Use Compliance

Employees shall complete and sign a 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 for special needs pursuant to state and federal law.

4.2.5.4 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 or his/her designee shall:

- Annually review a summary prepared by the KCTCS Vice-President responsible for Technology Solutions or his/her designee(s) 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 KCTCS 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 Vice-President for Technology Solutions shall recommend policies and procedures that ensure:

- That information within central repositories is secure and available.
- That information technology resources shared across KCTCS, including the communication network, are secure, available, and appropriately distributed.

Requests for exceptions to this policy shall be submitted for approval to the KCTCS President or his designee the KCTCS Vice-President responsible for Technology Solutions. All requests shall be submitted in written or electronic form.

In addition, the KCTCS Vice-President responsible for Technology Solutions shall:

- Annually review and forward to the KCTCS President any suggested modifications to this policy.
- Interpret this policy with advice of the KCTCS President and Cabinet officers.
- 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, KCTCS Vice President primarily responsible for Student Services, KCTCS Vice President primarily responsible for Human Resources, and the KCTCS Vice President primarily responsible for Finance shall:

- Assign a System Office designee within their respective areas with direct operational-level responsibility for information management of the records repository who will be responsible for data access, security and integrity, and policy implementation.

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.

- Assign a System Office designee within their respective areas with direct operational-level responsibility for information management of the records repository who will be responsible for data access, security and integrity, and policy implementation.

KCTCS Legal Services shall:

- Review local, state, and federal legislation for potential impact on this policy and its execution as needed.
- Make recommendations on the implementation of this policy and related procedures.
- Advise the KCTCS leadership on the legality of actions related to irresponsible use, including its investigation.

The system-level Information Security Officer shall:

- Serve as the primary contact for issues related to confidential and restricted information and information technology.
- Recommend rules, guidelines, and definitions for responsible use.
- Ensure that appropriate security controls are enabled and being followed in coordination with 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. (https://employees.kctcs.edu/ts/Pages/SecurityPolicy.aspx--click Data Classification Policy to view data classification type and element)
    - Administer policies and procedures for granting and maintaining access privileges for systems containing confidential or restricted information.

The system-level Senior Information Security Analyst shall:

- Serve as a primary resource for forensic analysis as it relates to confidential and restricted information and the support technology devices.
- Implement programs that support rules, guidelines and responsible use.
- In-depth analysis of potential vulnerabilities as it relates to information security throughout the KCTCS system.

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 and related procedures regularly to the academic community of the college.
- Identify problem areas to the KCTCS Vice-President 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.

The college-level Information Security Officer shall:

- Serve as the custodian of all information and information technology residing primarily at the college.

- 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. (https://employees.kctcs.edu/ts/Pages/SecurityPolicy.aspx--click Data Classification Policy to view data classification type and element)
    - Administer policies and procedures for granting and maintaining access privileges for systems containing confidential or restricted information.

The college senior administrator primarily responsible for information technology shall:

- Annually review and forward to the college president any suggested modifications to this policy.

4.2.5.5 Orientation Training, Ongoing Professional Training and Annual Compliance and Acceptance Review of Responsible Use of Information and Information Technology

All KCTCS employees shall:

- Complete basic web based security training; new employees shall complete training before access is granted to information resources.
- Review the requirements for responsible use of information and information technology annually and sign an acknowledgement statement either electronically or manually depending on the mode of delivery. Additional training may be required as best practices evolve.

Some KCTCS employees may be required to complete advanced training based on their level of access.

4.2.5.6 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.

4.2.5.6.1 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.
- Any unauthorized distribution of copyrighted material using KCTCS information technology resources is expressly forbidden.
- Using KCTCS network resources and technology in a peer to peer arrangement or internet downloading for the purpose of obtaining copyrighted materials (such as movies, music and literature) is forbidden in accordance with the *Higher Education Opportunity Act.*
- Communicating text or images using KCTCS information technology that is 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.
- Using or allowing use of information technology to access materials likely to be considered pornographic by institution leadership.

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/downloading on KCTCS information technology any unauthorized software which damages information or restricts the accessibility to the information technology resources (e.g. computer viruses, malware, spyware, etc.).
- Altering a communication of another individual without proper authorization.
- Altering existing information technology without proper authorization.
- Failing to provide the key to encrypted information or passwords to accounts that are needed during an investigation of irresponsible use.
- 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 unapproved mass emails, "spam", "chain letters", and indiscriminate use of "reply to all".

Courtesy

- 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.

4.2.5.6.2 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 addition, 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 through 434.860 (*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; 5-4-15	9-18-00; 6-21-06; 5-10-07; 5-20-08; 7-20-10; 11-2-10; 5-4-15	9-18-00; 6-21-06; 5-10-07; 5-20-08; 7-20-10; 11-2-10; 5-4-15
Approval Date	Date(s) of Last Review	Date(s) of Last Revision *(Include all dates in chronological order)*

(SIGNED)	5-4-15	(SIGNED)	5-4-15
Recommended by	Date	President, KCTCS	Date

4.2.6 Information and Information Technology Policy for Security Breaches and Suspected Security Breaches

This policy applies to data in electronic form and not to hard copies of same.

4.2.6.1 Definitions

Security Breach means when unencrypted confidential and restricted information of an individual is reasonably believed to have been acquired by an unauthorized person. Acquisition of Personal Information by a KCTCS employee or agent for bona fide KCTCS business purposes does not constitute a Security Breach, provided that the Personal Information is not used or subject to further unauthorized disclosure.

Security Breach Coordinator, for purposes of this Policy, is the individual or functional position to whom suspected Security Breaches are reported and with overall responsibility for ensuring compliance with this Policy, by his/her respective KCTCS college or functional area.

Suspected Security Breach means when a System containing Personal Information is, among other possibilities, lost or stolen, accessed in unauthorized fashion or infected by a virus or worm, but it is not yet known whether the Personal Information has been compromised to meet the level of a Security Breach.

System, for purposes of this policy, is any computer or computing device, including, but not limited to, desktops, laptops, PDAs, removable media such as CDs, USB flashdrives or iPods used as storage devices.

4.2.6.2 Responsibilities and Duties

College Presidents and KCTCS Vice Presidents must designate a Security Breach Coordinator and ensure that that individual reads this Policy and understands his/her responsibilities thereof. Changes to a designated Security Breach Coordinator must be approved by the appropriate official and communicated to system-level Information Security Officer.

Security Breach Coordinators are responsible for:

- Ensuring that all Suspected Security Breaches within their respective college, division or unit are investigated and reported to the KCTCS Chief Information Officer.
- Acting as liaison between their respective college, division or unit and the system-level Information Security Officer to facilitate investigation of such Suspected Security Breaches.
- Making arrangements for implementing notification requirements, including the actual distribution of notification letters or emails and the setting up of a hotline for inquiries if appropriate.

Other related duties and responsibilities may be assigned to a Security Breach Coordinator as deemed necessary.