

Computer Usage Policy For West Kentucky Community and Technical College (Revised September 2007)

5.2.1 Purpose and Intent

It is the purpose and intent of this policy to provide understanding and guidance for the responsible use of technology available on the West Kentucky Community and Technical College campus; to define the role of responsible use for all users and to guarantee computing resources for the students, faculty, staff and the community.

5.2.2 Policy Statements

5.2.2.1 General Policies

The computing resources at the West Kentucky Community and Technical College campus are divided into two areas: administrative or academic functions. Policies governing the administrative functions pertain to the usage of the KCTCS PeopleSoft System and any related KCTCS administrative software. Policies governing the academic functions pertain to the usage of the campus network; the KCTCS e-mail service, the Internet and the campus personal computer units. The West Kentucky Community and Technical College campus encourages the use of technology as a valuable resource for information and learning. The computing resources and services are to support the institutions academic and administrative goals.

5.2.2.1.1 Network / Email Access

The West Kentucky Community & Technical College network and the KCTCS network utilize an active directory security utility with Cisco Clean Access to provision network and e-mail access. Access to the campus network, KCTCS system network or e-mail service requires an active directory login ID and password.

Access, to the West Kentucky Community & Technical College campus network, is granted to an individual upon student enrollment, becoming an employee, designated as an affiliate of the college or through a temporary guest login. The PeopleSoft records system generates an active directory ID and e-mail address upon student enrollment. The PeopleSoft human resources module generates an employee ID and email address upon entry of employment records by the Human Resources Department. A student sets their password upon activating their e-mail address. New employees are required to present a photo ID to the Information Technology Department for the initial setup of their password. The automated active directory security utility requires employees and students to change their passwords every 90 days. Employees and students receive expiration notifications via e-mail 15 days prior to their password expiring. Community residents visiting the Library may obtain

a temporary guest login. Business and Industry training students who attend a one hour or one day training have access to systems only available to the Business and Industry training program for the hour/day in which they train.

5.2.2.2 Computing Policies for Administrative Functions

5.2.2.2.1 Access to Student Records

All staff and faculty who require access to the PeopleSoft system must submit a request to their supervisor or Dean, for approval by the appropriate Vice-President. A vice-president will submit the request to the KCTCS PeopleSoft System for the appropriate access. All employees and students entered into the PeopleSoft system have access to their self-service module. Upon termination of the employee, access to the self-service module is denied. Students only have access to their self service module while enrolled.

5.2.2.2.2 Confidentiality

All users of the PeopleSoft system will be made aware of the confidentiality practices adhered to at the college upon receiving access to the system. All users will follow the process governed by the Family Education Rights and Privacy Act of 1974 (FERPA). Records maintained by the college are available only to the student, KCTCS and community and technical college personnel with legitimate educational interests and to other institutions where the student is seeking financial aid. Copies of FERPA are available in Student Affairs.

All users of the PeopleSoft system are responsible for login and data confidentiality as listed in the KCTCS Administrative Policies and Procedures Section 4.2.5.3.

5.2.2.3 Computing Policies for Academic Functions

5.2.2.3.1 Freedom of Speech

The West Kentucky Community and Technical College campus upholds all measures of the Constitution of the United States. Upon the use of any computer on the West Kentucky Community and Technical College campus, the user accepts the 5 principles: Privacy, Lawfulness, Integrity of Information and Information Technology, Equitable Distribution of Information Technology and Courtesy outlined in the KCTCS Administrative Policies and Procedures Section 4.2.5.2.

5.2.2.3.2 Principles Governing the Use of Computing Resources

- Privacy - Confidentiality and Restricted Information
 - It is the responsibility of all users to protect confidential and restricted data. Individuals are “not” to share login ID’s or passwords. All students, employees, guests and affiliates are

responsible for ensuring the privacy of personal information about others.

- Lawfulness – Network services
 - The user may not use computer resources for any illegal or unauthorized act; in particular the user may not use computer resources to violate any state or federal laws or any of the regulations specified by West Kentucky Community & Technical College or KCTCS.
 - The user may not participate in any behavior that would interfere with the functionality of the West Kentucky Community & Technical College campus network.
 - Unauthorized accessing, using, copying, modifying or deleting of files, data, user ID's, access rights, usage records, or disk space allocations on any computer system is prohibited.
 - Copying or capturing licensed software for use on any system or by an individual for whom the software is not authorized or licensed is prohibited.
 - Downloading or uploading of Internet information or data that directly affects the operation of the campus network is prohibited.
- Integrity of Information and Information Technology
 - The technology devices are not to be ill-treated hindering reliability and performance.
- Equitable Distribution of Information Technology
 - It is the responsibility of the student, employee, guest, and affiliate to adhere to appropriate and fair use of information technology.
- Courtesy
 - Computer resources are contingent upon prudent and responsible use. It is the responsibility of the individual to maintain a professional and respectful environment when using technology on the West Kentucky Community & Technical College campus.
- Students, employees, guests and affiliates of West Kentucky Community & Technical College are responsible for the usage policies governed under KCTCS and the West Kentucky Community & Technical College. Examples of activities that are defined as violations reside in section 5.2.2.3.6 of this policy.

5.2.2.3.3 Student Usage

Personal computer systems are available for student use in designated computer labs and the campus library. Hours of availability are posted in the labs, library and on the campus web site. Students have the ability to utilize their own mobile computing devices in designated areas.

- Students are to use their Login ID and password for all computing areas on campus.
- Students are strongly discouraged from storing “personal” information on any campus computer.
- Students, employed through the student worker program, must present a photo ID to the Information Technology Department account administrators to reset a forgotten login password.
- WKCTC employees will not provide students with student ID or password information over the phone or via e-mail.
- Students of West Kentucky Community and Technical College are responsible for the 3.3.21 KCTCS E-mail Policy in regards to their KCTCS e-mail accounts.

5.2.2.3.4 Community Usage

Personal computer systems are available for community use in the campus library. It is the sole responsibility of each user to ensure they receive adequate instruction for using the computers through the library personnel.

5.2.2.3.5 Faculty / Staff Usage

It is the responsibility of all employees to safeguard confidential and restricted information from irresponsible use. All faculty and staff are required to take and pass a technology security test and record the results with the Human Resource Department.

E-mail Usage:

Faculty and staff of West Kentucky Community and Technical College are responsible for the 3.3.21 KCTCS E-mail Policy and the e-mail requirements listed below.

West Kentucky Community & Technical College e-mail directories used for distribution to all employees or the faculty and staff groups are for use by authorized personnel only. Internal spamming of the KCTCS E-mail system is prohibited. An e-mail is considered an "internal spam" e-mail when it is sent to mass groups and is not related to work issues. An example of an internal spam e-mail is sending an announcement of a new baby, a comical quote, announcing a great restaurant, Girl Scout cookie sales, etc., to all employees or a large group of employees.

To assist the campus in providing the best possible e-mail service, all e-mails announcing events, activities, fund raisers, etc., for the West Kentucky Community & Technical College campus should be sent to the Public Relations Department Daily E-mail Digest address WKCTCAnnouncements@kctcs.edu by 3 p.m. each day to be released the following morning. If you wish announcements to be sent to other colleges in the KCTCS system please include the information in your request to the Public Relations Department.

Academic Software, Network Data and Network Access:

Before updates, upgrades, or installations of new or existing academic software can be completed on the campus network servers all software, licenses, manuals and related materials as well as a work order request, must be delivered to the Information Technology Department one month prior to the start of a semester. The Information Technology Department will provide a software request form to all faculty.

A security access request form must be submitted for approval to the Information Technology Director for access to any folder, data, or objects stored on the campus servers, other than the home folders. Security access request forms may be obtained upon request from the Information Technology Department.

Requests for remote access to the campus network, which includes; campus servers, switches, workstations, printers or any other device, not designated as “public access” by Director of Information Technology must be submitted in writing by the supervisor to the Director of Information Technology for approval. Remote access “not” approved by the Director of Information Technology and the President of the college is considered unauthorized and is in violation of this policy.

5.2.2.3.5.1 Faculty / Staff Web Publishing

- All websites must be approved by the Director of Information Technology, Director of Public Relations, and Vice-President of Learning Initiatives prior to implementation.
- The hosting location for distance learning courses is recommended for faculty web sites or the hosting location for the campus web site should be used.
- The distance learning software used for Internet courses is recommended for course related web sites.
- Individual units acting as web servers are prohibited without the written approval of the Director of Information Technology and the Vice-President of Learning Initiatives.
- FTP (File Transfer Protocol) services acting as remote access to individual non-public units on campus is prohibited and falls under the remote access requirements. A user’s supervisor must submit in writing a request for remote access, which must have approval by the Director of Information Technology and the Vice-President of Learning Initiatives prior to implementation.
- All requests for web sites by faculty and staff members must be submitted in writing by a supervisor or Dean to the Vice President of Learning Initiatives. The Vice President of Learning Initiatives will review the request with the Director of Information Technology and will approve or disapprove the concept of the website. The proposed website with concept

approval will be submitted to the Director of Public Relations for consideration. Approved staff web sites will be hosted at the campus web site host location.

- Web site domain names are to be approved by the Director of Public Relations and the President.

5.2.2.3.6 Activities Defined as Examples of Violations

KCTCS and West Kentucky Community and Technical College have defined the following activities as unacceptable use. All violations of these principles or any attempt to violate these principles constitutes misuse. Violations include those found in the KCTCS Administrative Policies and Procedures defined in 4.2.5.8.1 and those shown below but 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 classroom/lab or publicly accessible computer logged on but unattended by the user.
 - Transferring confidential or restricted data to non-KCTCS devices including home computers, removable memory devices and personal digital devices without authorization.
 - Accessing another individual's personal e-mail or files without their specific permission is gross misconduct.
- **Lawfulness**
 - Use of the Internet or e-mail for personal gain, or personal business activities as defined in a commercial sense such as buying or selling commodities or services with a profit motive.
 - Use of the Internet or e-mail for unlawful activities.
 - Misrepresentation of oneself or the Commonwealth.
 - Copying, moving, capturing license software for use on a system for which the software was not licensed or for use by an individual for which the software is not authorized.
 - Intentional obscuring or forging of the date, time, physical source, logical source, or other header information of a message or transaction.
 - Interception of transmitted information.
 - Disseminating, copying or printing copyrighted materials (including articles, videos, audio and software) in violation of copyright laws.

- **Integrity of Information and Information Technology**
 - Unauthorized accessing, using, copying, modifying, or deleting of files, data, user ID's, access rights, usage records or disk space allocations.
 - Accessing resources for purposes other than those in which the access was originally issued, including inappropriate use of authority or special privileges.
 - Use of computing resources for remote activities that are unauthorized.
 - Individual units acting as a web server without the written approval of the Vice-President of Learning Initiatives and Information Technology Director.
 - Causing computer failure through an intentional attempt to "crash the system" or through the intentional introduction of a program that is intended to subvert a system such as a worm or virus.
 - Other activities that could cause congestion and disruption of networks and systems; i.e., spam mail, downloading audio or video files not related to work or curriculum can cause network congestion.

- **Equitable Distribution of Information Technology**
 - Intentionally wasting information technology resources, including central processing unit time, storage, network capacity, printing resources and related supplies.
 - Using information technology for non-WKCTC related purposes on a routine or extended basis.
 - Creating or sending communications which may overload the network including, chain letters, spam, etc.

- **Courtesy**
 - Knowingly and repeatedly visiting pornographic or illegal sites for disseminating and soliciting sexually oriented messages or images.
 - Soliciting money for religious or political causes, or advocating religious or political opinions.
 - Use of abusive or objectionable language in either public or private e-mail messages.

5.2.2.3.7 Responses to Violations

Per 4.2.5.8.2 of the KCTCS Administrative Policies and Procedures:

For a student found to have made irresponsible use of information or information technology on the WKCTC campus, 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, West Kentucky Community & Technical College and KCTCS may require the individual to reimburse the campus for computing and personal 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 434.840 (*Unlawful access to a computer*) may be referred to the Commonwealth Attorney or 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.

<u>9/20/2007</u>	<u>August 2006</u>	Ruby Rodgers	
Approval Date	Date of Last Revision	Info. Tech. Director	<u>9/2007</u>
		Recommended By	Date

<u>(signed)</u>	<u>9/2007</u>
President/CEO West Kentucky Community and Technical College	Date