PELLISSIPPI STATE COMMUNITY COLLEGE

**POLICY 08:13:05**
**COMPUTER SYSTEM USE**

## I. Purpose

The purpose of this policy is to define the appropriate use and procedures for using college-owned or -operated computing resources to protect the security and integrity of the resource, data and network.

## II. Scope and Applicability

This policy applies to any employee, student visitor, client or guest of the college who uses any provided college-owned or -operated computing resource. All faculty, students, staff, and guests are responsible for the use of Pellissippi State's computing resources in an effective, efficient, ethical and lawful manner. The following guidelines relate to the use of these computing resources. Additional requirements and procedures may be required for the authorized use of specific college computing laboratories. (Any additional requirements or procedures will be posted in the respective laboratories.)

Computing resources and accounts are owned by the College and are to be used only for college-related activities that support the mission, goals and purposes of the College. All access to the College's computer systems must be approved and approvals may require displaying of proper identification or completion of forms when requested. Access to departmental computer systems must be approved by the dean, the director, the department head or an authorized representative; approvals vary depending upon the unit. Only college-owned or college-approved equipment may be attached to the local wired network. All other computers and devices are to connect only through the campus wireless network unless approved by the director of Networking and Technical Services and follow Pellissippi State Policy No. 08:13:06 Bring Your Own Device (BYOD).

## III. Risks, Liabilities, Disclaimers

The College makes available computing facilities consisting of hardware, software, accounts and communication activities. The College accepts no responsibility for any loss of data or damage to data or services arising directly or indirectly from the use of these facilities or for any consequential loss or damage. The College makes no warranty, express or implied, regarding the computing services offered or their fitness for any particular purpose.

## IV. Policy and User Responsibilities

1. Regular faculty and staff, temporary faculty and staff, and students who have been admitted to the College are considered eligible for computer accounts.
2. An account password for email accounts and other server-based resources can be overridden when necessary by authorized administrators, including the employee's supervisor. The vice president of Student Affairs may authorize an override of a student account.
3. Disciplinary actions will conform with other college policies and may result in a disciplinary review conducted by the vice president of Student Affairs, or designee, in matters involving alleged violations by students, or by the director of Human Resources in matters involving employees of the College.
4. An individual's computer use privileges may be suspended immediately upon the discovery of a

possible violation of this policy, other campus policies or illegal activities. The director of Network and Technical Services, the vice president of Student Affairs, or designee, or the director of Human Resources will judge an offense as either major or minor. A first minor offense will normally be dealt with by the director of Network and Technical Services and/or an appropriate supervisor. Major or additional minor offenses will be forwarded to the appropriate vice president. The account may be removed, deactivated or have privileges removed from one or all college computing systems permanently or until the matter is completely resolved.

5. The College will make reasonable efforts to maintain the integrity and effective operation of its computer systems, including electronic mail, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature of technology, the College can assure neither the privacy of an individual user's use of the College's computer system resources nor the confidentiality of particular messages that may be created, transmitted, received or stored thereby. In addition, communications of college personnel that are sent by electronic mail constitute "correspondence" and, therefore, will be considered public record subject to public inspection under Section 6 of the Public Records Act TCA 3-12-105. Tennessee's public records law requires that computer files be treated as open records. Additionally, files in user accounts are subject to the discovery process or subpoena. Email is stored as files and is therefore subject to the same rules and restrictions as any other files. Additionally, email is very easy to forward, and any email sent can easily become a matter of general dissemination. Forwarding email from an account at the College to a private account with an Internet Services Provider may make the private account subject to the same potential for discovery and subpoena during legal actions as is the account at the College.

6. The College will not monitor electronic mail as a routine matter, but it may do so to the extent permitted by law as the College deems necessary for purposes of maintaining the integrity and effective operation of the College's electronic mail system.

7. The College reserves the right to inspect and disclose the contents of electronic mail:

    i. in the course of an investigation triggered by indications of misconduct or misuse;

    ii. as needed to protect health and safety of the college community;

    iii. as needed to prevent interference with the academic mission; or

    iv. as needed to locate substantive information required for college business that is not more readily available by some other means.

It is each individual user's responsibility to abide by the following:

1. Computing resources and accounts are to be used only for the purpose for which they were assigned and are not to be used for commercial purposes or non-college-related activities. The prohibition against commercial or non-college-related purposes also applies to World Wide Web pages written and published from any Pellissippi State user account and to advertisements of products and services or links to advertisements and services on commercial World Wide Web pages from Pellissippi State user Web pages (see Pellissippi State Policy No. 08:13:04, World Wide Web (WWW) Page Development And Use).

2. All accounts, including student user accounts, assigned to an individual, must not be used by others. Faculty, students and staff are individually responsible for the proper use of their accounts, including proper password protection and appropriate use of Internet resources. Allowing friends, family or coworkers to use accounts, either locally or through the Internet, is a serious violation of these guidelines. Courtesy accounts may only be authorized when they are related to official college business and activities. (Instructions for obtaining courtesy accounts are explained in Pellissippi State Policy 08:13:02 Computer Account Policy.) Faculty, students and staff are responsible for choosing an appropriate password that is difficult to guess. If an individual suspects his/her account password has been compromised, he/she should change the password immediately.

3. Passwords, keyboard locking software, or other security measures that are based on individual computers or devices rather than on servers cannot be as easily overridden. Therefore, they may be used only with the permission of a supervisor and only if the supervisor is provided with the password or other unlocking mechanism.
4. User account passwords may be reset by the owner using the password reset utility provided on the HelpDesk website.
5. Users may use programs and files only in their own accounts, unless the programs and files have been explicitly (either by written approval or security systems) made available to others by the custodian of the data. Seeking to gain unauthorized access to files and programs in someone else's account is a serious violation of this policy.

6. Users should understand that rules and regulations that apply to other forms of communications at the College also apply to email. In addition, the following specific actions and uses of College email are improper:
   i. concealment or misrepresentation of names or affiliations in email messages;
   ii. alteration of source or destination address of email messages;
   iii. use of email for commercial or private business purposes;
   iv. use of email to impede, hinder or otherwise affect email, network and other technical services;
   v. use of email to harass or threaten other individuals;
   vi. use of email that violates the student code of conduct; or
   vii. use of email that violates copyright, libel, or defamation laws

7. Software use must conform to copyright laws and licensing agreements. Software is protected by copyright law whether or not a copyright notice is explicitly stated in the software or in its documentation. It is illegal to make duplicate copies of a single software product unless authorized to do so by the author or publisher of the software product. Computer users have no rights to give or receive duplicates of software without authorization or to install software onto college computing equipment. Software installation may only be performed by authorized personnel.

8. Computing systems staff cooperate with instructors to detect and verify plagiarism using computer systems, software and programs. In order to discourage plagiarism, students should be sure to pick up and/or discard all printed output.

9. Users may not attempt to circumvent security, to use knowledge of loopholes in computer system security or unauthorized knowledge of a password to damage or disrupt any computing systems or college network, to obtain extra computing resources, to take resources from another user, or to gain access to unauthorized computing systems, files or programs - either on or off campus. Any of these attempts is a violation of these guidelines.

10. No one should deliberately attempt to degrade the performance of a computer system (including network resources) or to deprive authorized users of resources or access to any college computer system. When a process is consuming excessive system resources or objectionably degrading system response, it may be terminated or its priority may be altered without notice.

11. Faculty, students, or staff that suspect violation of system or application security must contact the HelpDesk immediately so that appropriate actions can be taken. Faculty, students, or staff not following the Computer System Use policy must be reported immediately to the director of Network and Technical Services for appropriate action.

Approved: President Allen G. Edwards, June 16, 1998
Approved: President Allen G. Edwards, August 23, 1999
Approved: President Allen G. Edwards, August 19, 2002
Approved: President Allen G. Edwards, October 21, 2002
Approved: President Allen G. Edwards, June 7, 2004
Reviewed/Recommended: President's Staff, August 21, 2006
Approved: President Allen G. Edwards, August 21, 2006
Reviewed/Recommended: President's Staff, April 14, 2008
Approved: President Allen G. Edwards, April 14, 2008
Editorial Changes, July 2008, July 1, 2009
Reviewed/Recommended: President's Staff, October 5, 2009
Approved: President Allen G. Edwards, October 5, 2009
Reviewed/Recommended: President's Council, May 19, 2014
Approved: President L. Anthony Wise, Jr., May 19, 2014
Reviewed/Recommended: President's Council, Nov. 21, 2016
Approved: President L. Anthony Wise Jr., Nov. 21, 2016
Reviewed/Recommended: President's Council, February 19, 2018
Approved: President L. Anthony Wise, Jr., February 19, 2018