PELLISSIPPI STATE COMMUNITY COLLEGE

POLICY 08:13:01
INFORMATION TECHNOLOGY ACCEPTABLE USE

I. Purpose

The purpose of this policy is to define the appropriate use and procedures for using College-owned or -provided computing systems, accounts, and other technology resources to protect the security and integrity of the resource, data and network.

II. Scope and Applicability

This policy applies to all individuals using or attempting to use any computer or information technology resource of the College.

This policy applies to all computing, technology and data resources and accounts owned and/or provided by the College and used for college-related activities that support the mission, goals and purposes of the College. All parties with access to data on the college network or stored by the college should be familiar with this policy

Non-College owned or provided computers and devices must also follow Pellissippi State Policy No. 08:13:06 Bring Your Own Device (BYOD).

III. Risks and Liabilities

The College makes available computing systems and resources consisting of hardware, software, accounts and communication activities. The College makes no warranty, express or implied, regarding the computing services offered or their fitness for any particular purpose. The College will not be responsible for any damages, including loss of data resulting from delays, non-deliveries, or service interruptions caused by user negligence, errors or omissions.

Use of a computer or information technology resource or system signifies the following:

- The user accepts responsibility for knowing the contents of this policy statement. Failure to read or acknowledge this statement will not be an excuse for noncompliance.

- The user accepts that failure to comply with this policy may result in temporary or permanent denial of access to computer or information technologies, or in some cases may result in college disciplinary action or legal action.

Policy and User Responsibilities

Pellissippi State Community College will ensure the confidentiality, integrity, and availability of technology and data through the development and implementation of compliance standards which address security requirements and expectations for acceptable use of computer systems. These standards will follow industry-defined best practices in securing technology and data.

Users must comply with Tennessee Board of Regents Policy 1:08:00:00 Information Technology Resources and Policy No 1.08.05.00 IT Acceptable Uses.

Access to College technology resources such as, but not limited to, computing equipment, telecommunications, network services, servers, software, applications, information resources, printing and scanning services, and user and technical support provided by Information Services staff is a privilege, not a right. Regular faculty and staff, temporary faculty and staff, and students who have been admitted to the College are considered eligible for computer accounts. Every personal account will be assigned to an individual and must not be shared. Guests of the college requiring access may request a courtesy account when required for official college business and activities. The process for requesting and assigning accounts is in Pellissippi State Policy 08:13:02 Computer Account Policy.

Every personal and service account will be assigned a unique password and/or other authorization factor. Users must not share their password(s) with another person. 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.

The College will make reasonable efforts to maintain the integrity and effective operation of its electronic communications 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 and electronic records, including electronic mail, are subject to inspection and records requests.

Users may use programs and files only in their own accounts, unless the programs and files have been explicitly made available to others by the custodian of the data, either by written approval following Policy 08:13:08 Electronic Account Access or by other security systems. Seeking to gain unauthorized access to files and programs in someone else's account is a serious violation of this policy.

Users should understand that rules and regulations that apply to other forms of communications at the College also apply to email. 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. Communications of college personnel that are sent by electronic mail may be considered public record subject to public inspection under the Tennessee Public Records Act T.C.A. § 10-7-501 et seq.

Additionally, files in user accounts are subject to the discovery process or subpoena.

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(s). In addition, the College reserves the right to inspect and disclose the contents of electronic mail:

- in the course of an investigation triggered by indications of misconduct or misuse;
- as needed to protect health and safety of the college community;
- as needed to prevent interference with the academic mission; or
- as needed to locate substantive information required for college business that is not more readily available by some other means.

The following specific actions and uses of College email or other information resources are improper:

- concealment or misrepresentation of names or affiliations;
- alteration of source or destination address of email messages;
- for commercial or private business purposes;
- for political purposes;

to impede, hinder or otherwise affect email, network and other technical services;

to harass or threaten other individuals;

to violate the student code of conduct; or

to violate copyright, libel, or defamation laws

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. As a recognized agent under the Digital Millennium Copyright Act, the College will act in accord with the provisions of this act in the event of notification of alleged copyright infringement by any user.

Information Services staff may cooperate with instructors and other College officials to detect and verify plagiarism using computer systems, software and programs.

a. User Responsibilities

As a user of Pellissippi State Community College's technology resources, you have a shared responsibility with the College Information Services staff to maintain the integrity, confidentiality and availability of our systems, services, and data. Your responsibilities include the following:

All information technology use must comply with the provisions of this Acceptable Use Policy as well as Tennessee Board of Regents Policy 1.08.05.00 IT Acceptable Users.

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, College-Related Website Development and Use for more information. Personal software is not supported on college-owned machines.

All individually assigned accounts, including student user accounts, must not be used by others. Faculty, students and staff are individually responsible for the proper use of their accounts, including proper password creation and protection and appropriate use of Internet resources. If an individual suspects his/her account password has been compromised, he/she should change the password immediately.

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.

Employees are responsible for the protection of information on college-owned computers assigned to them. Users should choose the appropriate location and security for storing sensitive or other work-related information. If information needs to be shared, it should be placed on a server or college approved cloud service and protected by a password unique to each user. Only network drives have backup procedures in place and are configured with appropriate security controls. Users should be aware that local drives of college-owned computer systems and devices are not backed up by College technical staff.

Account owners who use laptops, peripheral storage or other mobile devices to access or store information defined as confidential or restricted by Policy 08:13:13 Data Classification must ensure the device is encrypted and protected by a passcode or biometric security. All college-owned mobile devices must be registered with Information Services.

Anyone who uses a college provided account on a personal and/or mobile device to access college e-mail or other data resources must abide by Policy 08:13:06 Bring Your Own Device (BYOD).

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 this policy.

System users shall not 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.

Faculty, students, or staff that suspect violation of this policy or of any system, application, or data security must contact the HelpDesk immediately so that appropriate actions can be taken.

IV. Enforcement

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.

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. Any offense that results in suspected or real compromise of confidential or restricted data will be brought to the incident response team as part of the College's Cyber Incident Response Plan.

Approved: President's Council, November 14, 1994
Approved: President Allen G. Edwards, December 17, 2001
Approved: President Allen G. Edwards, May 3, 2004
Reviewed/Recommended: President's Staff, February 16, 2009
Approved: President Allen G. Edwards, February 16, 2009
Reviewed/Recommended: President's Staff, August 17, 2009
Approved: President Allen G. Edwards, August 17, 2009
Reviewed/Recommended: President's Staff, March 22, 2010
Approved: President Allen G. Edwards, March 22, 2010
Reviewed/Recommended: President's Council, May 19, 2014
Approved: President L. Anthony Wise, Jr., May 19, 2014
Policy 08:13:01 was formally titled Computer Usage, title changed to
Information Technology Acceptable Use, September 9, 2019
Reviewed/Recommended: President's Council, September 9, 2019
Approved: President L. Anthony Wise, Jr., September 9, 2019