2.23 Technology Resources Acceptable Use

Last Revised: July 2023

Policy: Piedmont Community College's (PCC) information systems and the data contained therein are owned by the College and provided solely to support the educational mission of PCC for authorized users only. All employees, students, and others in the user community are expected to act responsibly and in conformity with generally accepted rules of network etiquette.

Purpose/Definitions:

Purpose

The purpose of this policy is to define the unacceptable uses of PCC's information technology systems or resources. This policy describes the types of network applications that are contrary to the College's network mission, and which are therefore prohibited. These are guidelines only and are not meant to be an exhaustive list of prohibited activities.

Definitions

AUP—Acceptable Use Policy

Information Technology Services (ITS)—the acronym used to designate Information Technology Services.

Plagiarism—"the wrongful act of taking the product of another person's mind and presenting it as one's own" (Alexander Lindey, Plagiarism and Originality, 1952).

User—any person that is not ITS personnel that has been assigned a valid active directory logon by ITS. Such logons (or accounts) should be used only by the owner of the account in a legal and ethical fashion.

Approval Authority/Monitoring Authority: Piedmont Community College's Board of Trustees has approval authority for this policy. The Vice President, Administrative Services/CFO has monitoring authority for this policy.

Procedure:

Section 1: Network Mission

1.1. The network, and through the network the Internet, offers an abundance of educational material as well as opportunities for collaboration and the exchange of ideas and information.

1.2. PCC recognizes the educational value of the Internet, and strongly encourages the responsible use of the network by all users.

1.3. Successful operation requires that all users view the network as a shared resource, and work together to maintain its integrity by behaving in a responsible, conscientious manner.

Section 2: Privacy Rights and Security

2.1. User data files, email, and electronic storage areas are considered the property of PCC, subject to the College's control and inspection.

2.1.1. The appropriate ITS administrator may access all such files and communications to ensure system integrity and that users are complying with the requirements of this regulation and any associated regulations.

2.1.2. Users should not expect that information stored on the network will be private.

2.2. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account.

2.2.1. Under no conditions should a user provide their password to another person.

2.2.2. Users will immediately notify ITS if they have identified a possible security problem relating to misappropriated passwords.

Section 3: Prohibited Use

3.1. Illegal or Destructive Activities

3.1.1. Users may not use the network for any purpose that violates the law or threatens the integrity of the network or individual workstations. Prohibited activities include, but are not limited to:

3.1.1.1. Attempting to gain unauthorized access to the network or go beyond their authorized access.

3.1.1.1.1. This includes attempting to log on through another person's account, generic account or access another person's files, attempting to obtain passwords, or attempting to remove any existing network security functions.

3.1.1.1.2. Users will not actively search for security problems, because this will be construed as an illegal attempt to gain access.

3.1.1.2. Intentionally developing or using programs to harass other users or to attempt to violate the security or alter software components of any other network, service, or system.

3.1.1.2.1. Examples of such activities include hacking, cracking into, monitoring or using systems without authorization, scanning ports, conducting denial-of-service attacks, and distributing viruses or other harmful software.

3.1.1.3. Attempting to damage hardware, software, or data belonging to the College or other users.

3.1.1.3.1. This includes adding, altering, or deleting files or programs on local or network hard drives and removing or damaging equipment such as mice, projectors, motherboards, speakers, or printers.

3.1.1.4. Fraudulent use of credit card numbers to purchase online merchandise.

3.1.1.5. Connecting or disconnecting any hardware to the network that has not been pre-approved by ITS.

3.1.1.6. Distributing or downloading licensed software or installing software such as games or music in violation of software license agreements (piracy).

3.1.1.6.1. This includes any peer-to-peer file sharing.

3.2. Inappropriate Material

3.2.1. Users will not use the network to access or distribute material that is obscene, indecent, hateful, advocates illegal acts, or advocates violence or discrimination toward other people.

3.2.1.1. This includes but is not restricted to distribution through email, discussion groups, or web pages.

3.3. Respect for Other Users

3.3.1. Restrictions against inappropriate language or images apply to personal email, discussion group postings, and material posted on web pages.

3.3.1.1. Users will not use obscene, profane, vulgar, inflammatory, threatening, or disrespectful language.

3.3.1.2. Users will not post false, defamatory, or derogatory information about a person or organization, or information that, if acted upon, could cause damage to individuals or property.

3.3.2. Users will not harass other persons through the network.

3.3.2.1. Such harassment includes, but is not limited to, distribution of unsolicited advertising, chain letters, or email spamming (sending an annoying or unnecessary message to a large number of people).

3.3.2.2. Users will not post personal contact information about other people, including address, telephone, home address, work address, etc.

3.3.2.3. Users must not send mail that does not accurately identify the sender, the sender's return email address, and the email address of origin.

3.4. Resource Limits

3.4.1. No software shall be downloaded from the Internet or email on a workstation without prior permission from ITS personnel.

3.4.1.1. Software installed by any user other than ITS personnel is considered a violation of this regulation without prior consent.

3.4.1.2. Users have a right to temporary use of disk storage space and are responsible for keeping their disk usage below the maximum size allocated.

3.4.1.3. Long term storage of large video files should be stored on the user's OneDrive.

3.4.1.4. Extremely large files, if left on the network for an extended period, may be removed at the discretion of the Vice President, Information Technology/CIO.

3.4.2. Users will check their email frequently.

3.4.2.1. Where applicable, users will comply with state and federal statutes governing public record retention. (See PCC Policy 5.7.1 Employee Personnel File, Section 3, for additional information.)

3.4.3. Users are to utilize college email for the purposes related to the College and performance of their jobs, but incidental personal use is allowed.

3.4.3.1. Use of college technology, including email accounts, is limited to purposes related to the College and to employees' job performance.

3.4.3.2. Use of college technology for private financial gain, advertising, solicitation or fund-raising for any non-college purpose will be considered a violation of this regulation unless approved by the President.

3.4.4. Theft of Intellectual Property

3.4.4.1. Users must respect the legal protection provided by copyright law and license agreements related to content, text, music, computer software and any other protected materials. (For additional information, see PCC Policies 2.16 Copyright and Fair Use Policy and 2.16.1 Intellectual Property)

3.4.4.1.1. Users will not plagiarize works that they find on the Internet.

3.4.4.2. Users will respect the rights of copyright owners.

3.4.4.2.1. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright.

3.4.4.2.2. If a work contains language that specifies Technology Resources Acceptable Use of that work, the user shall follow the expressed requirements.

3.4.4.2.3. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

3.4.4.2.4. It is the regulation of PCC that any illegal peer-to-peer file sharing over the College's network is prohibited.

3.4.4.2.5. Unauthorized distribution of copyrighted material, such as through peer-to-peer networks, may subject users to civil and criminal penalties.

3.4.4.2.6. Federal law authorizes a copyright owner to recover civil damages.

3.4.4.2.6.1. Copyright infringement may also be criminally prosecuted.

Section 4: Virus & Ransomware Protection

4.1. To maintain a secure and reliable computing environment within our campus, PCC requires all computers connected to the network, or that could be connected to the network, to have a reliable and updated anti-virus scan program on each computer.

4.1.1. This program must be updated and scans performed on a regular basis.

4.1.2. ITS shall maintain network-level anti-virus protection on college owned devices.

4.1.3. Any person who knowingly introduces a virus, worm, ransomware, or Trojan horse programs onto any computer or server is subject to disciplinary action, including restitution. (See PCC Policy 5.19 Employee Disciplinary Policy and/or Policy 7.5 Code of Conduct for more information.)

Section 5: Security Awareness

5.1. All users who have access to computers, email, or other forms of electronic data must acknowledge that they have read and agree to comply with all PCC policies and procedures adopted by ITS.

5.2. Employees are required to take a security awareness class annually.

Section 6: Username and Password

6.1. PCC requires all employees and students be properly identified and authenticated before being allowed to access the college network.

6.2. Users are responsible for safeguarding their passwords and are responsible for all transactions using their passwords.

6.2.1. No individual may assign their account or password to any other person.

6.2.1.1. Any person who deliberately makes their account available to an unauthorized user will incur termination of their account.

6.2.1.2. Similarly, any person who fraudulently gains access to another person's password or account may incur disciplinary action. (See PCC Policy 5.19 Employee Disciplinary Policy and/or Policy 7.5 Code of Conduct for more information.)

Section 7: Network Security

7.1. Any and all actions that jeopardize the integrity and stability of the network by violating the network security standards outlined in this policy or any other college policy is subject to disciplinary action commensurate to the level of risk or damage incurred. (See PCC Policy 5.19 Employee Disciplinary Policy and/or Policy 7.5 Code of Conduct for more information.)

Section 8: Access

8.1. Users who are given authorization may connect to the college network, for college activities through a wired or wireless connection after demonstrating compliance with security procedures established by ITS.

Section 9: Remote Access

9.1. This policy refers to connection to the college computing network from outside of the PCC network, such as from a user's home.

9.2. The computer systems, networks and data repositories of the College's network are critical resources and must be protected against unauthorized access, malicious access, and disruption of service.

9.2.1. Authorized users of the College's computer systems, networks and data repositories may be permitted to remotely connect to those systems, networks and data repositories for the conduct of college related business only through secure, authenticated and carefully managed access methods.

Section 10: Technology Hardware and Software Procurement

10.1. To maintain high levels of reliability, cost effectiveness, and interoperability of the communications and data technology within the College, PCC requires all technology purchases, with the exception of toner/ink cartridges, be approved by ITS.

Section 11: Student Information System

11.1. PCC maintains a database system for a wide variety of information management purposes.

11.1.1. Much of the information is personal information on students, faculty, employees, alumnae and friends of the College.

11.1.2. PCC considers the security of this information to be one of the College's most serious responsibilities, and accordingly, access to these databases is limited to persons who have a legitimate need to use the information to advance the academic and administrative goals of the College.

11.2. Persons who are given passwords and have legitimate access to the information on Ellucian Colleague / Banner have a strict responsibility to ensure that this information is used appropriately, and that the privacy of persons identified through this information is strictly protected. (See PCC Policy 5.7.1 Employee Personnel File and Policy 7.6 The Family Educational Rights and Privacy Act of 1974 for more information.)

11.2.1. This responsibility extends both to information available on computer screens as well as information available in print media, including all printouts, manual dossiers, correspondence files, directories, and similar forms of information banks.

Section 12: Telephone System and Voicemail

12.1. PCC provides telephone and voicemail access to many employees.

12.1.1. The same policies and expectations that govern e-mail also govern voicemail and telephone usage.

12.2. Any use of PCC telephones for any fraudulent or illegal purpose will incur severe penalties, including the possible involvement of law enforcement authorities as well as disciplinary action by the College. (See PCC Policy 5.19 Employee Disciplinary Policy and/or Policy 7.5 Code of Conduct for more information.)

12.3. Telephone misconduct includes misuse of telephone credit cards, misuse of college long-distance access codes, theft of telephone instruments, and any related misconduct.

Section 13: Violation of this Regulation

13.1. In the event there is an allegation that a user has violated this policy, the user will be provided with notice of the alleged violation and an opportunity to present an explanation before an administrator.

13.1.1. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student or employee in gaining the self-discipline necessary to behave appropriately on a computer network. (See PCC Policy 5.19

Employee Disciplinary Policy and/or Policy 7.5 Code of Conduct for more information.)

13.1.2. The Vice President, Information Technology/CIO has authority to disable any account where there is a violation of this policy.

13.2. The College may at its sole discretion determine whether a use of the network is a violation of this policy.

13.2.1. Violations of this policy may result in a demand for immediate removal of offending material, blocked access, suspension or termination of the users account, or other action appropriate to the violation.

13.2.2. The College reserves the right to act without notice, when necessary, as determined by the administration.

13.2.3. The College may involve, and will cooperate with, law enforcement officials if criminal activity is suspected.

13.2.3.1. Violators may also be subject to civil or criminal liability under applicable law.

Legal Citation: N.C.G.S. 115D-24 , N.C.G.S. 132

History: Effective October 2001; revised April 2009, January 2011, May 2021, July 2023

Cross-references PCC Policies 2.16 Copyright and Fair Use Policy, 2.16.1 Intellectual Property, 5.7.1 Employee Personnel File, 5.19 Employee Disciplinary Policy, 7.5 Code of Conduct, 7.6 The Family Educational Rights and Privacy Act of 1974