Pitt Community College
Information Technology Resources

Appropriate Use Policy

Overview

The primary purpose of the Pitt Community College computer resource is educational. The College's mission is to educate and empower people for success. This mission will be achieved by encouraging lifelong learning, establishing positive learning environments, ensuring academic excellence, enhancing economic development and quality of life, and emphasizing multicultural experiences. All users must understand this purpose.

This policy applies to the use of cellular and landline telephones, radios, voice mail systems and Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, and internet access. These systems are to be used in the course of normal operations to support the mission of the College.

Effective security is a team effort involving the participation and support of faculty, staff and students as they manage access to information and/or information systems. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of technology resources provided by Pitt Community College. These rules are in place to protect student privacy and state resources. Inappropriate use exposes Pitt Community College to risks including:

- virus attacks
- compromise of network systems and services
- legal issues
- financial consequences
- negative publicity and trust within the community

Users violating guidelines, including applicable state and federal laws, are subject to loss of network privileges. In addition, violation of state or federal statutes could make the users subject to criminal prosecution.

The PCC Information Technology Resources Acceptable Use Policy will be distributed to all employees and all students. It will be posted electronically on PCC's computers which are available for use by the general public and students. It will be available during new student orientation materials and the PCC General Catalog.

It is the user's responsibility to read and abide by the topics set forth in this and other related documents. This policy will be made available and should be reviewed by all employees and students as part of an orientation session.

Scope

This policy applies to employees, students, contractors, consultants, temporaries, and other workers for Pitt Community College, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Pitt Community College.

Policy

I. General Use and Ownership

a) While Pitt Community College's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create remains the property of Pitt Community College.

b) The encryption of sensitive or vulnerable information stored on any portable device is mandatory.

c) For security and network maintenance purposes, authorized individuals within Pitt Community College may monitor equipment, systems and network traffic at any time.

d) Pitt Community College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

II. Security and Proprietary Information

a) The user interface should be classified as confidential. Users shall take all necessary steps to prevent unauthorized access to this information.

b) Remote access to computing resources will be protected by multi-factor authentication methods to ensure that access to resources including our distance learning platform is restricted to the person who is enrolled in the class.

c) Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

d) All administrative PCs, laptops and workstations will be secured with a password-protected screensaver with automatic logging-off when the host is unattended for a specific period of time.

e) Information contained on portable computers is especially vulnerable, so special care should be exercised and loss of such equipment will be made to the OITS Department immediately.

f) All hosts used by the employee that are connected to the Pitt Community College administrative network shall be continually executing approved virus-scanning software with a current virus database, unless overridden by group policy.

g) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

III. Expectations of Personal Privacy

There should be no “expectation of personal privacy” in the usage of Pitt Community College Information Technology resources, in fact, Pitt Community College reserves the full right to access, monitor, retrieve and disclose any digital information that has been stored or transmitted, to or from any technology resource that is owned or leased by Pitt Community College without advance notice. The Pitt Community College Information Technology Director or his/her delegate may exercise his/her right to access under, but not limited to, the following: (1) impropriety, (2) violation of college policy, (3) legal requirements, (4) suspected criminal activities, (5) breach of system security.

IV. Acceptable and Unacceptable Usage

The users of all PCC's computer resources, and computer network must rely on the honesty, integrity, and respect for the rights of others and on a conscious effort to be of service to others and the community. Users are advised that technology are business tools that shall be used in a **professional manner only** at all times and should not be used for any purpose, which would reflect negatively on the College or its employees. The College does not attempt to define all acceptable or unacceptable uses of the network. Acceptable conduct must be assessed by individual users. The following information assists the users in making such assessments.

a) Uses that are **acceptable and encouraged**:

1) Access to scientific, technical, and other informational topics as well as conducting communication among peers in other government agencies, academia and industry on matters which have relevance to Pitt Community College
2) Communications and information exchanges directly relating to the mission, charter and work tasks of the College
3) Announcements of College policies, meetings, procedures, services, or activities
4) Obtaining and spreading knowledge
5) Gathering research material and data
6) Analyzing research material and data
7) Providing data and research in support of public service
8) Preparing course materials
9) Enhancing educational approaches and teaching methods
10) Enhancing course work
11) Developing surveys and administering targeted demographic surveys

b) Uses that are **unacceptable and punishable**:

1) Users are responsible for their actions and activities including responsibility for becoming informed of and complying with license and copyright provisions of the software they use. Unacceptable use of computing resources will result in suspension or revocation of those privileges

I. It is unacceptable for a user to access, use, submit, publish, display, download, save, or transmit on the network, or on any computer system, any information which:

II. Violates or infringes on the rights of any other person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Pitt Community College.

III. Contains illegal, defamatory, misleading, inaccurate, false, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, biased, or otherwise discriminatory material;

IV. Restricts, derogates or disrupts any college resource's performance adversely affecting daily operations, other users or the Internet, or misrepresent the interests of the college.

V. Encourages the use of controlled substances or uses the system for the purpose of criminal intent; or any other illegal purpose.

2) Sending unsolicited email messages, “Junk Mail” or other advertising materials including “chain letters”, inappropriate jokes or similar type emails (spam).
3) Data that is in violation of copyright infringement of any local, state or federal law.
4) Creating, installing or distributing unauthorized or malicious software.
5) Gaining or allowing access to others to restricted technology resources (Sharing passwords).
6) Using, storing or transferring *Copyrighted* information (The Federal Copyright Act, U.S.C. Title § 17-106) including plagiarism.
7) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Pitt Community College or the end user does not have an active license is strictly prohibited.
8) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
9) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
10) Using a Pitt Community College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
11) Making fraudulent offers of products, items, or services originating from any Pitt Community College account.
12) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
13) Port scanning or security scanning is expressly prohibited.
14) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
15) Circumventing user authentication or security of any host, network or account.
16) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
17) Text Messaging, must be conducted in accordance with all applicable laws and require the active consent, opt-in of recipients for non-emergency messages.
18) Using technology for financial or other commercial gain;
19) Vandalizing the data of another user;
20) Wastefully using finite resources;

21) To ensure that the student who registers in a distance or correspondence education course or program is the same student who participates in and completes the course or program and receives the credit, it is unacceptable for anyone else to gain access to resources or entities by impersonating another user;

22) Invading the privacy of individuals;

23) Posting anonymous messages which incite, inflame, and are derogatory or the intent is malice;

24) Creating and displaying threatening, obscene, racist, sexist, or harassing (persistently annoying of another user) material, including broadcasting unsolicited messages or sending unwanted mail;

25) Using the network in support of groups outside the College when such use is not in keeping with the mission of the College;

26) Using personal web pages not primarily focused on the mission of the College.

c) It is also ***unacceptable*** for a user to use the features and capabilities of the System to:

27) Knowingly open information or e-mails not directed to you (unless under direction of the Information Owner).

28) Utilizing unauthorized removable storage devices.

29) Gaining or allowing access to others to restricted areas within the physical facilities

30) (including "*piggybacking*" on another employee's access badge).

31) Conducting any non-approved business such as:

I. Any activity or unauthorized purchases that is prohibited by law;

II. Any activity for used for personal gain or personal business including Commercial ventures, political causes or other non-job-related solicitations including non-College-related fund raising or public relations activities.

V. Manners

Appropriate network manners include being polite, using appropriate language, and not revealing personal addresses or phones numbers of students or colleagues. Remember: Electronic mail (email) is not guaranteed to be private. In addition, system operators log network use (www, e-mail, etc.). However, all communication and information accessible on the networks can be assumed to be private (following the dictates of common politeness and common sense).

VI. Authorization

Students, faculty, and staff must have appropriate authorization to use computing resources.

VII. Disclaimer

Information obtained through www.pittcc.edu is at the user's own risk. PCC is not responsible for the accuracy or quality of information obtained. Users need to consider the source of any information obtained, and, as this is a global network, accept responsibility for accessing inappropriate material as described under Unacceptable Uses.

VIII. Policy Agreement

As a condition of employment, all Pitt Community College employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties accessing the Pitt Community College network must sign the Acceptable Use Policy Acknowledgement Form acknowledging that they understand the terms of this policy and the proper usage of the Pitt Community College Information Technology Systems as well as the potential punitive actions for non-compliance. Furthermore, all Pitt Community College employees must accept this policy.

Immediately upon implementation of this policy, supervisors will review this policy with all new workers. Human Resources will provide a copy of the policy to applicable new hires, collect, and maintain the signed agreement forms in the Human Resources Department. The Office of Information Technology Services (OITS) will receive the signed Request for Access (RACS) forms as part of the on-boarding process. Access to Pitt Community College systems will only be allowed upon receiving confirmation of signed documents.

IX. Policy Enforcement

This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the technology resources provided by the College and are not necessarily exhaustive.

Questions about specific uses should be directed to the AVP Of Information Technology and Services.

It is in the responsibility of all users to **exercise good judgment** and maintain a **professional manner** while utilizing the Pitt Community College's technology resources as well as report any violations to their supervisor or directly to the Helpdesk.

Policy Contact Information

Any questions related to the above can be directed to Ernest Simons, AVP Information Technology & Services, (252)493-7243 or by email elsimons352@my.pittcc.edu.