COMPUTER USE AND ELECTRONIC COMMUNICATION POLICY

Pittsburgh Technical College (PTC) has established this policy with regard to the use of college provided computer equipment, software, copiers, network, phone system, and both wired and wireless Internet connections (collectively referred to as the "PTC system.")

This policy includes all general-purpose use of the PTC system. In addition, it covers activities using the Internet and the use, access, and disclosure of electronic communication including but not limited to messages, audio and video, photographic or digitally created images, documents, and other information which can be created, sent, or received using the PTC system.

The use of the PTC system is intended for authorized activities such as educational and business activities at PTC. Personal use should be kept to a minimum. This policy is applicable at all times, which includes class time, work time, break time, after hours and on weekends, and applies whether the user is on or off PTC premises during use of the system. The PTC system hardware is college property; all data composed, sent, or received using the system remain the property of PTC and are not the private property of any user.

In this policy **"authorized user"** includes any student or employee of PTC who uses and/or participates in the use of, the system as it is defined above. In addition, **"customer"** is defined as any parent, student, vendor, or other person(s) engaged in business with PTC.

ENFORCEMENT

PTC will enforce the policies set forth below and reserves the right to add to, modify, or delete them at any time as may be required under prevailing circumstances. Violations of this policy will be subject to the highest forms of discipline, up to and including termination. In addition, any user(s) who engage in negligent, willful, or deliberate acts which result in damage to the system will be held financially liable for that damage and any residual effects associated with those act(s). Noncompliance with these policies could result in termination of employment, suspension, or expulsion from PTC.

USER PRIVACY

The PTC system is for use only by authorized users. There is no right to privacy for anyone using this system. PTC has the right to monitor and record user activities of the PTC system which may be provided to police or other law enforcement organizations for reasons including criminal invsetigation. Unauthorized or illegal activities on the system may be punishable by law.

USER RESTRICTIONS

PTC's information resources must be protected in a manner consistent with its sensitivity and criticality. All users are responsible for using the PTC system and Internet appropriately and in an effective, ethical, and lawful manner.

PROHIBITED ACTIVITIES

PTC prohibits the PTC system from being used to create illegal or discriminatory materials or messages. Materials or messages containing disparaging and/or discriminatory content, or which offensively address someone's age, race, ethnicity, color, religion, national origin, disability, veteran status, sexual orientation, sex, gender identity, genetic information, or any other protected category under applicable local, state, or federal law are prohibited.

Also prohibited are messages which are fraudulent, harassing, obscene, or which are intended to instill fear and those which contain abusive, profane or offensive language.

Users shall not use a code to access or attempt to access a communication file, or retrieve any stored communications data on the PTC system unless authorized to do so. If an employee user changes jobs (including termination, transfer, promotion, or leave of absence) the Human Resources Department (HR) will inform IT to make any necessary changes to access rights. If access to another user's data is needed, a request to the HR must be made and then forwarded to the IT Department.

PTC has the right to determine what constitutes appropriate use of the system and the Internet. Prohibited uses include, but may not be limited to the following:

1. Use for illegal activity or extensive use for other non-school related purposes.
2. Use for advertising, commercial, and/or profitable purposes.

3. Use to order or purchase any merchandise or services in the name of PTC, unless authorized, and/or any individual.
4. Use for academic dishonesty.
5. Use for political lobbying.
6. Use for religious causes.
7. Use of hate mail, discriminatory remarks, fear-mongering, and/or offensive or inflammatory communication.
8. Installation, distribution, reproduction, and/or use of copyrighted materials without permission of the copyright holder.
9. Use to access or download obscene or pornographic material.
10. Use of inappropriate language and/or profanity.
11. Use to transmit material offensive and/or objectionable to the recipient.
12. The impersonation of another user and/or use of anonymity and pseudonyms.
13. Loading, downloading, or use of unauthorized games, program files, or other electronic media to devices provided by the college. All software must be approved and installed by the IT Department.
14. Destruction, modification, or abuse of networks, hardware, and/or software.
15. Allowing an unauthorized person to use an assigned computer or account.
16. Sharing PTC provided login information, passwords, or other login credentials with anyone. This includes but is not limited to college owned systems.
17. Unauthorized hacking into any computer system, including college systems and network equipment. Authorization-related to PTC systems may only be granted in writing by the Chief Information Officer (CIO).
18. Engaging in any form of cyberbullying.
19. International and toll calls for non-business purposes.

REQUIREMENTS

PTC requires that all users:

1. Use cryptic passwords that cannot be easily guessed and protect the passwords
2. Participate in required data security and privacy training
3. Protect information resources when using internet and email
4. Secure physical area before leaving area unattended
5. Lock or log off of computers or other devices when not in use
6. Secure memory sticks
7. Keep file cabinets containing Confidential or Internal Use Only information locked when not in use or when unattended
8. Paper printouts containing Confidential or Internal Use Only information must be removed immediately from printers
9. Paper copies of Confidential or Internal Use Only documents should be properly disposed of using designated receptacles to ensure the information is shredded.
10. Whiteboards containing Confidential or Internal Use Only should be erased when no longer needed but until then hidden from public view.

FAIR USE OF COPYRIGHT

Copyrighted materials or trade secrets belonging to entities other than this college may be used only for legitimate and lawful purposes. PTC has adopted a Fair Use Policy (PTC Student Handbook), which outlines what uses may be made of copyrighted material. Users are not permitted to copy, transfer, rename, add or delete data or programs belonging to others unless given express permission to do so by the owner, except in compliance with the Fair Use Policy. Failure to observe the copyright laws, the Fair Use Policy, or license agreements may result in disciplinary action by the college and legal action by the copyright owner.

Any persons who discover a violation of this policy shall notify the IT Department or HR.

SOCIAL MEDIA

The information that employees post on public social media, including Facebook, Twitter, YouTube, LinkedIn, blogs, and special interest forums, reflects on them and how they represent PTC. The same inappropriate content policy that applies to the Internet generally applies with equal force to social media. Time at work spent on personal social media sites must be kept to a minimum. Social media sites may be monitored by PTC without permission of the author. The college will take action to posts referencing PTC if they are inappropriate. See the college's Social Media Policy (PTC Policy Manual).

PERSONAL MOBILE DEVICES

The use of personal devices (mobile, tablet, laptop, etc.) at PTC should be limited as to not negatively impact work productivity, the student experience, assigned responsibilities, and team or individual projects.

To keep from bothering or distracting others, employees should set cell phones to vibrate or silent mode. Making or taking phone calls near others, or using the speakerphone function should be avoided.

PTC-PROVIDED COMMUNICATIONS EQUIPMENT

The PTC will issue a mobile device to employees including faculty and staff whose work requires that he/she be immediately or readily reachable by PTC. The same policies outlined above apply to anyone who is issued a PTC mobile device. Equipment can be used for reasonable personal use, as long as the employee complies with all associated PTC policies.

IMPROPER USE OF PTC ISSUED MOBILE DEVICES

Use of PTC issued mobile devices is prohibited during the operation of a motor vehicle, machinery, heavy machinery, or when the use of any other equipment/device could lead to the injury or death of the user or others. Use common sense while driving or operating machinery.

Employees must pull over and stop the vehicle in a safe location prior to making or receiving a cell phone call, or when sending or viewing received text messages or email communications. If operating machinery, take the proper steps to stop the machine and step away.

Employees who are ticketed for a traffic violation because he/she used a PTC

issued mobile device while driving will be fully responsible for any fines and/or penalties incurred, and will be subject to disciplinary action by PTC.

Video or Audio Recording Devices

Faculty, staff, and students must use their best judgment when recording video or audio anywhere on PTC property (both on- and off-campus). Recording audio in the state of Pennsylvania without permission of all parties being recorded is illegal (PA Wiretapping Law). Recording others without their knowledge may be construed as an invasion of privacy and/or harassment. In addition, recordings may reveal PTC's confidential or protected information, which is in violation of PTC policy.

Lost, Stolen, or Damaged Personal Equipment

PTC cannot and will not be responsible for any loss, theft or damage to personal mobile devices or other personal property brought to the college.

Maintenance of Personal Equipment

PTC cannot and will not be responsible for technical support of personal devices. Support of hardware and software on personal devices is solely the responsibility of the owner. By request, the IT Department may provide recommended third-party vendors to assist employees and students. The college is not responsible for any loss, damage, or costs associated with the aforementioned recommendations.

Friends and Family

It is the responsibility of PTC employees and students to ensure that family members and friends know and respect this policy. No one, other than the designated user, should use PTC issued equipment for any purpose.

PTC Owned Data on Personal Mobile Devices

Employees who do not have a PTC issued mobile device are able to add PTC email accounts, contact lists, calendar, and internal portals to her/his device in compliance with PTC policy and with the approval of the IT department.

The college is able to separate PTC data from personal data by incorporating mobile device management (MDM) solutions, which offers a way to separate personal information from business data on mobile devices. If a user loses

her/his mobile device or leaves the employ of PTC, the business data can be removed remotely.

Personal devices that store PTC owned data, messages, or software must have MDM software installed. Upon leaving PTC, employees must coordinate the deletion of all college-owned data, messages, and software with the IT Department.