Pennsylvania College of Technology

Policy Statement

Title: Information Technology Resources Acceptable Use Policy	**Number:** P 8.03
Approved by: Presidential Action	**Approved Date:** 11/01/2022 **Implementation Date:** 11/01/2022 **Last Review Date:** 11/2022 **Last Revision Date:** 11/2022

Persons/Departments Affected:

All employees, students, and other individuals accessing or utilizing College IT (Information Technology) resources

Responsible Department:

Information Technology Services

Definitions:

Classification: Process of organizing and identifying organizational information to relevant categories to be protected more efficiently, facilitate appropriate access, and maintaining regulatory compliance. Penn College utilizes the following three categories. For more information see P8.04\Data Classification.

I. Public: Information whose loss, corruption, or unauthorized disclosure would cause minimal or no personal, financial, or reputational harm to the institution, institution staff or the constituents/people we serve.

II. Private: Information whose loss, corruption, or unauthorized disclosure would likely cause limited personal, financial, or reputational harm to the institution, institution staff or the constituents/people we serve.

III. Restricted: Information whose loss, corruption, or unauthorized disclosure would cause severe personal, financial, or reputational harm to the institution, institution staff or the constituents/people we serve.

Policy:

I. PURPOSE

Pennsylvania College of Technology (Penn College)'s technology infrastructure exists to support the academic and administrative activities needed to fulfill the institution's mission. Access to these resources is a privilege that should be exercised responsibly, ethically, and lawfully.

The purpose of this Acceptable Use Policy is to clearly establish each member of the institution's role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives will enable Penn College to implement a comprehensive system-wide Information Security Program.

II. SCOPE

This policy applies to all users of computing resources owned, managed, or otherwise provided by the institution. Individuals covered by this policy include, but are not limited to all students, faculty, staff, student workers and service providers with access to the institution's computing resources and/or facilities. Computing resources include all Penn College-owned, licensed, or managed hardware and software, email, and web domains and related services and any use of the institution's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

III. PRIVACY

Penn College will make every reasonable effort to respect a user's privacy. However, users do not acquire a right of privacy for communications transmitted or stored on the institution's resources. Additionally, in response to a judicial order or any other action required by law or permitted by official Penn College policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the institution, the President of the institution may authorize a Penn College official or an authorized agent, to access, review, monitor and/or disclose computer files associated with an individual's account. Examples of situations where the exercise of this authority would be warranted include, but are not limited to, the investigation of violations of law or the institution's rules, regulations, or policy, or when access is considered necessary to conduct Penn College business due to the unexpected absence of faculty, staff, or student workers or to respond to health or safety emergencies.

IV. POLICY

Activities related to Penn College's mission take precedence over computing pursuits of a more personal or recreational nature. Any use that disrupts the institution's mission is prohibited.

Following the same standards of common sense, courtesy and civility that govern the use of other shared facilities, acceptable use of information technology resources generally respects all individuals' privacy, but subject to the right of individuals to be free from intimidation, harassment, and unwarranted annoyance. All users of Penn College's computing resources must adhere to the requirements enumerated below as well as other College Policies and Procedures.

A. FRAUDULENT AND ILLEGAL USE

Penn College explicitly prohibits the use of any College information system or network resources for fraudulent and/or illegal purposes. While using any of the institution's information systems or network resources, a user must not engage in any activity that is illegal under local, state, federal, and/or international law. As a part of this policy, users must not:

i. Violate the rights of any individual or company involving information 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 Penn College.

ii. Use in any way copyrighted material including, but not limited to, photographs, books, or other copyrighted sources, copyrighted music, and any copyrighted software for which the institution does not have a legal license. See P7.17\Copyright Policy and PR7.17\Copyright Procedure for details.

iii. Export software, technical information, encryption software, or technology in violation of international or regional export control laws.

iv. Issue statements about warranty, expressed or implied, unless it is a part of normal job duties, or make fraudulent offers of products, items, and/or services.

Any user that suspects or is aware of the occurrence of any activity described in this section, or any other activity they believe may be fraudulent or illegal, must notify his/her supervisor immediately.

If any user creates any liability on behalf of Penn College due to inappropriate use of the institution’s resources, the user agrees to indemnify and hold the institution harmless, should it be necessary for Penn College to defend itself legally against the activities or actions of the user.

B. CONFIDENTIAL INFORMATION

Penn College has both an ethical and legal responsibility for protecting confidential information classified as “Restricted” or “Private” in accordance with P8.04\Data Classification. To that end, there are some general positions that the institution has taken:

Transmission of confidential information by unauthorized end-user messaging technologies (for example, personal e-mail accounts, instant messaging, SMS, chat, etc.) is prohibited.

The writing or storage of confidential information on mobile devices (phones, tablets, USB drives) and removable media is prohibited. Mobile devices that access confidential information will be physically secured when not in use and located to minimize the risk of unauthorized access.

All faculty, staff, student workers and service providers will only use approved devices to access confidential institutional data, systems, or networks. Noninstitutionally owned devices that store, process, transmit, or access Private or Restricted information is prohibited. Accessing, storage, or processing Private or Restricted information on personal computers owned devices is prohibited, except via virtual desktop provided by PCT.

All institution portable devices will be securely maintained when in the possession of workforce members. Such devices will be handled as carry-on (hand) baggage on public transport. They will be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile) when not in use.

Photographic, video, audio, or other recording equipment will not be utilized in designated secure areas.

All confidential information stored on devices must be encrypted by Penn College Information Technology Services.

All students, faculty, staff, and student workers who use institution-owned devices will take all reasonable precautions to protect the confidentiality, integrity and availability of information contained on the workstation.

Institution faculty, staff, student workers and affiliates who move electronic media or information systems containing confidential information are responsible for the subsequent use of such items and will take all appropriate and reasonable actions to protect them against damage, theft and unauthorized use.

Institution workforce members will activate their device locking software whenever they leave their device unattended or will log off from or lock their device when their shift or usage is complete.

C. HARRASSMENT

Penn College is committed to providing a safe and productive environment, free from harassment, for all faculty, staff, and student workers. For this reason, users must not:

i. Use institution information systems to harass any other person via e-mail, telephone, or any other means, or
ii. Actively procure or transmit material that is in violation of sexual harassment or hostile workplace laws.

If a user feels they are being harassed through the use of the institution’s information systems, the user must report it, in writing, to their supervisor or any department head.

D. INCIDENT REPORTING

Penn College is committed to responding to security incidents involving personnel, institution-owned information, or institution-owned information assets. As part of this policy:

The loss, theft, or inappropriate use of institution access credentials (e.g., passwords, key cards, or security tokens), assets (e.g., laptop, cell phones), or other information will be immediately reported to the IT Service Desk.

No student, faculty, staff, or student worker will prevent another member from reporting a security incident.

E. MALICIOUS ACTIVITY

Penn College strictly prohibits the use of information systems for malicious activity against other users, the institution's information systems themselves, or the information assets of other parties.

i. DENIAL OF SERVICE

Users must not:

a. Perpetrate, cause, or in any way enable disruption of Penn College's information systems or network communications by denial-of-service methods.
b. Knowingly introduce malicious programs, such as viruses, worms, and Trojan horses, to any information system; or
c. Intentionally develop or use programs to infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.

Exceptions for approved academic purposes may be granted by ITS through a formal agreement.

ii. CONFIDENTIALITY

Users must not:

a. Perpetrate, cause, or in any way enable security breaches, including, but not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access.
b. Facilitate use or access by non-authorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends.
c. Use the same password for Penn College accounts as for other non-Penn College access (for example, personal ISP account, social media, benefits, email, etc.).
d. Attempt to gain access to files and resources to which they have not been granted permission, whether such access is technically possible, including attempting to obtain, obtaining, and/or using another user's password.
e. Make copies of another user's files without that user's knowledge and consent.

All encryption keys used on PCT equipment employed by users must be provided to Information Technology if requested, to perform functions required by this policy.

Base passwords on something that can be easily guessed or obtained using personal information (e.g., names, favorite sports teams, etc.).

iii. IMPERSONATION

Users must not:

a. Circumvent the user authentication or security of any information system.
b. Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information.
c. Create and/or use a proxy server of any kind, other than those provided by Penn College, or otherwise redirect network traffic outside of normal routing with authorization; or
d. Use any type of technology designed to mask, hide, or modify their identity or activities electronically.

F. NETWORK DISCOVERY

Users must not:

i. Use a port scanning tool targeting either Penn College's network or any other external network, unless this activity is a part of the user's normal job functions, such as a member of Information Technology Services conducting a vulnerability scan, or faculty utilizing tools in a controlled environment.
ii. Use a network monitoring tool or perform any kind of network monitoring that will intercept data not intended for the users unless this activity is a part of the user's normal job functions.

G. OBJECTIONABLE CONTENT

Penn College strictly prohibits the use of the institution's administrative information systems for accessing or distributing content that other users may find objectionable. Users must not post, upload, download, or display messages, photos, images, sound files, text files, video files, newsletters, or related materials considered to be:

i. Political
ii. Racist
iii. Sexually explicit
iv. Violent or promoting violence

H. HARDWARE AND SOFTWARE

Users may not install, attach, connect, remove, or disconnect hardware of any kind, including wireless access points, storage devices, and peripherals, to any institution information system without the knowledge and permission of Information Technology Services.

Penn College strictly prohibits the administrative or academic use of any hardware or software that is not purchased, installed, configured, tracked, and managed by the institution.

Users must not:

1. i. Install, attach, connect, remove, or disconnect hardware of any kind, including wireless access points, storage devices, and peripherals, to any institution information system without the knowledge and permission of Information Technology Services.
2. ii. Download, install, disable, remove, or uninstall software of any kind, including patches of existing software, to any institution information system without the knowledge and permission of the institution.
3. iii. Use personal flash drives, or other USB based storage media, without prior approval from their manager; or
4. iv. Take Penn College equipment off-site without prior authorization.

I. MESSAGING

The institution provides a robust communication platform for users to fulfill its mission.

Users must not:

1. i. Send unsolicited electronic messages, including “junk mail” or other advertising material to individuals who did not specifically request such material (spam).
2. ii. Solicit electronic messages for any other digital identifier (e.g., e-mail address, social handle, etc.), other than that of the poster's account, with the intent to harass or to collect replies; or
3. iii. Create or forward chain letters or messages, including those that promote “pyramid” schemes of any type.

Employees must not:

1. i. Automatically forward electronic messages of any kind, by using client message handling rules or any other mechanism.

J. REMOTE WORKING AND TELECOMMUTING

When working remotely or telecommuting, users must adhere to Policy P3.03.38 \Telecommuting and Procedure PR3.03.38\Telecommuting.

Be given explicit approval per the above linked policy and procedure.

Safeguard and protect any institution-owned or managed computing asset (e.g., laptops and cell phones) to prevent loss or theft.

Not utilize personally owned computing devices for Penn College work including transferring Penn College Information to personally owned devices without approval per the above linked policy and procedure.

Take reasonable precautions to prevent unauthorized parties from utilizing computing assets or viewing Penn College information processed, stored, or transmitted on institution-owned assets.

Not create or permanently store private or restricted information on local machines. Temporary copies may be stored while working but should be deleted from local storage as soon as is practicable.

Not access or process confidential information in public places or over public, insecure networks without proper encrypted communication by only using approved methods for connecting to the institution (e.g., VPN, remote desktop).

K. OTHER

College-provided IT resources are primarily designated for instructional, research, or administrative purposes. Employees and students may use these resources for personal purposes if that use does not interfere with the primary use and does not interfere with one's normal duties and responsibilities. Users must not use the institution's information systems for commercial use or personal gain.

L. PROVISIONS FOR PRIVATE COMPUTERS CONNECTED TO THE COLLEGE NETWORK

The following apply to anyone connecting a private computer to the College network.

The owner of the computer is responsible for the actions of all users on the computer, and all network traffic to and from the computer, whether the owner is aware of it or not.

A private computer connected to the network may not be used to provide network access for anyone who is not authorized to use the College systems. The private computer may not be used as a router or bridge between the College network and external networks, such as those of an Internet Service Provider (ISP).

In the event ITS staff have any reason to believe that a private computer connected to the College network is using the resources inappropriately, network traffic to and from that computer will be monitored. If justified, the system will be disconnected from the network, and action will be taken by the appropriate authorities.

Any student with an authorized network account may use the College's network, as long as the usage

i. does not violate any law, regulation, or this policy
ii. does not involve extraordinarily high utilization of college resources or substantially interfere with the performance of the College network
iii. does not result in commercial gain or profit
iv. is not in violation of any part of this policy

Users are responsible for the security and integrity of their systems. In cases where a connected device is compromised, the user shall shut down the system and remove it from the campus network as soon as possible to localize any potential damage and to stop the attack from spreading. If you suspect electronic intrusion or that your device/system has been compromised and would like assistance, contact the IT Service Desk at 570-329-4848 or e-mail ITServiceDesk@pct.edu immediately

Personal servers and network equipment should never be connected to the Penn College network without prior authorization from Information Technology Services.

V. ROLES AND RESPONSIBILITIES

PCT reserves the right to protect, repair, and maintain the institution's computing equipment and network integrity. In accomplishing this goal, Penn College ITS personnel or their agents must do their utmost to maintain user privacy, including the content of personal files and Internet activities. Any information obtained by ITS personnel about a user through routine maintenance of the institution's computing equipment or network should remain confidential, unless the information pertains to activities that are not compliant with acceptable use of PCT's computing resources.

VI. ENFORCEMENT

Enforcement is the responsibility of the institution's President or designee. Users who violate this policy may be denied access to the institution resources and may be subject to penalties and disciplinary action both within and outside of Penn College. The institution may temporarily suspend or block access to an account, prior to the initiation or completion of disciplinary procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the institution or other computing resources or to protect Penn College from liability.

Users are subject to disciplinary rules described in policies and procedures governing acceptable workplace behavior.

VII. EXCEPTIONS

Exceptions to the policy may be granted by the Vice President for Information Technology and Chief Information Officer, or by their designee. All exceptions must be reviewed annually.

VIII. INDEMNIFICATION/LIABILITY STATEMENT

A. The Pennsylvania College of Technology makes absolutely no warranties of any kind, either express or implied, for the Internet services it provides. The College will not be responsible for any damages suffered by users, including, but not limited to, any loss of data resulting from delays, non-deliveries, user errors, or service interruptions.

B. The College is not responsible for the accuracy or quality of information obtained through its Internet services, including e-mail. Users assume responsibility for any damages suffered as a result of information obtained through these sources.

C. The user agrees to indemnify and hold harmless Pennsylvania College of Technology, the Board of Directors, and College employees from and against any claim, lawsuit, cause of action, damage judgment, loss, expense, or liability resulting from any claim, including reasonable attorneys' fees, arising out of or related to the use of the College's hardware, software, and network facilities. This indemnity shall include, without limitation, those claims based on trademark or service mark infringement, trade name infringement, copyright infringement, defamation, unlawful discrimination or harassment, rights of publicity, and invasion of privacy.

IX. REFERENCES

The Gramm - Leach Bliley Act (GLBA)
Family Educational Rights and Privacy Act (FERPA)
Pennsylvania's Breach of Personal Information Notification Act
NIST 800-53
FIPS-199
PCI DSS 3.1
Code of Ethics of the American Library Association

Revision History:

Date:
Date:
Date:

Cross References:

Information Security Policy P8.02
Data Classification Policy P8.04