Purpose: To define what constitutes acceptable and responsible use of the information and communication technology resources of the Pennsylvania College of Health Sciences.

Scope

This policy applies to all faculty, staff, students, and trusted third parties of PA College. This policy applies to the use of PA College data/information, PA College assets, and PA College network resources, whether owned or leased by PA College, the user, or a third party. All faculty, staff, students, and trusted third parties of the PA College its subsidiaries are responsible for exercising good judgment regarding appropriate use of data/information, electronic devices, and network resources in accordance with PA College policies and standards, and local laws and regulation.

Definitions

Access

Having the ability to read, edit, modify, and/or delete data and information.

Confidentiality

Keeping data and information private. This means that only accounts that have access to the specific data and information can see and work with it.

Integrity

Keeping data and information consistent and uncorrupted.

Availability

Having the data and information when it is needed.

PA College system

Any device, application, cloud-based system, or other product that PA College owns or licenses.

Policy

Pennsylvania College of Health Sciences is an institution of higher education, dedicated to education, scholarship and the pursuit of knowledge. It is not the intent of this policy to impose restrictions that are contrary to PA College's established culture of openness, trust and integrity. There is a commitment to protecting members of the PA College community and the College as a whole from illegal or damaging actions by individuals, either knowingly or unknowingly.

PA College assets, services, data/information, and systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations.

Effective security is a team effort involving the participation and support of every member of the PA College community and affiliates who deal with data and information and/or information systems. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

Users of PA College's information and communication technology resources have access to sensitive data/information and external networks. Consequently, it is important that they use these resources in a responsible, ethical and legal manner. Inappropriate use of these resources threatens the atmosphere for the sharing of information, the free exchange of ideas and the security of an environment for creating and maintaining information resources. In general, acceptable use means an accountable, rational and appropriate exercise of a freedom to use while respecting the rights of other computer users, the integrity of the College's data/information and communication technology resources and all pertinent license and contractual agreements.

General Use and Ownership Responsibilities

PA College proprietary data/information stored on electronic and computing devices whether owned or leased by PA College, a member of the PA College community or a third party, remains the sole property of PA College. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Security of Data and Information Policy* in conjunction with the *Security of Data and Information Standards.*

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of PA College proprietary information, or any PA College assets you are in possession of.

You may access, use, or share PA College proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

All PA College faculty, staff, students, and trusted third parties are responsible for exercising good judgement and operate within good faith.

Individual departments dictate the guidelines for personal use of PA College systems. It is the responsibility of the user for exercising good judgement regarding reasonableness of personal use. Where there is uncertainty, users should consult their direct report.

For security and network maintenance purposes, authorized individuals within PA College may monitor equipment, systems, and network traffic at any time. For more detail on this, please reference the *Privacy of Data and Information Policy*.

PA College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Unacceptable Use

The following activities are, in general, prohibited. Select staff may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., ITS systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is a user of PA College systems authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing PA College owned resources. The following list (as well as those provided in forthcoming sections) is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

- Violations of the rights of any 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 PA College.
- Presenting materials as academic work, submitted electronically or otherwise, that indicate plagiarism or other form(s) of academic dishonesty.
- 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 PA College or the end user does not have an active license is strictly prohibited.
- Impersonation of a PA College resource, employee, student, or trusted third party in order to misrepresent the College. Users are strictly prohibited from using the PA College name or its likeliness to create personal accounts and from using personal accounts to conduct PA College business.
- Accessing data/information, a system, or an account for any purpose other than conducting necessary PA College business or for acceptable allowed personal use, even if you have authorized access, is prohibited.
- PA College resources may not be used for commercial purposes except only as permitted with explicit prior written approval of the Offices of Academic Affairs.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs/code into the network or server (e.g. viruses, worms, Trojan horses, etc.)
- Revealing your account password/passphrase or use of the account to others. Never share your password/passphrase with others or enter it anywhere that you have not verified as a trusted PA College system.
- Using a PA 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.

- Making fraudulent offers of products, items, or services originating from any PA College account.
- Making statements about warranty, expressly or implied, unless it is normal job duties.
- Effecting security incidents, breaches, or disruptions of network communication. For more information on security incidents or breaches, please see the *Security of Data and Information Policy*.
- 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.
- Port scanning or IT network security scanning is expressly prohibited unless prior notification to the PA College Department of Information Technology Services (ITS) is made and the scanning activity is approved by ITS.
- Executing any form of network monitoring which will intercept data/information not intended for the user's host (the PA College asset used by the individual), unless this activity is part of the user's normal job/duty.
- Circumventing user authentication or security of any PA College asset, account, or network
- Introducing honeypots, honey nets, or similar technology on or to the PA College network.
- Interfering with or denying service to any user other than that user's host.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, PA College employees to parties outside PA College (i.e. PA College directory information).
- Place bets, wagers, or operate games of chance.
- Transmit or make accessible material, which in the sole judgment of the College is offensive, violent, pornographic, annoying or harassing, including use of PA College's information systems to access and/or distribute obscene or sexually explicit material.
- Using the College's resources to misrepresent or impersonate someone else.
- Generate and/or spread intolerant or hateful material, which in the sole judgment of the College is directed against any individual or group, based on race, religion, national origin, ethnicity, age, gender, marital status, sexual orientation, veteran status, genetic makeup, or disability.

Email and Communication Activities

When using PA College resources to access and use the Internet, users must realize they represent the company. Whenever members of the PA College community state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the PA College Department of Information Technology

Services. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use of PA College email and communication resources:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use or foraging of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within PA College's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by PA College or connected via PA College's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Online Conduct

In addition to the items outlined below, PA College employees are held accountable under the policies of Penn Medicine Lancaster General Health regarding online conduct, including but not limited to the Penn Medicine Lancaster General Health Social Media Policy and the Penn Medicine Lancaster General Health Media Relations Policy. PA College students are held accountable to Student Code of Conduct, outlined in the Student Handbook.

Online conduct, including but not limited to blogging, posting on social media sites, or posting on discussion boards, by employees, whether using PA College's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of PA College's systems to engage in online conduct is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate PA College's policy, is not detrimental to PA College's best interests, and does not interfere with an employee's regular work duties. Online conduct from PA College's systems is also subject to monitoring.

The *Security of Data and Information Policy* also applies to online conduct. As such, Employees are prohibited from revealing any PA College confidential or proprietary information, trade secrets or any other material covered by *Security of Data and Information Policy* or *Security of Data and Information Standards* when engaged in online conduct.

Users shall not engage in any online conduct that may harm or tarnish the image, reputation and/or goodwill of PA College and/or any members of PA College's community. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments through online conduct or

otherwise engaging in any conduct prohibited by PA College's Discrimination and Harassment administrative policy statement. Students are held to the conduct standards outlined within the Student Handbook.

Users also may not attribute personal statements, opinions or beliefs to PA College when engaged in online conduct. If an employee is expressing his or her beliefs and/or opinions online, the user may not, expressly or implicitly, represent themselves as an employee or representative of PA College. Users assume any and all risk associated with online conduct.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, PA College's trademarks, logos and any other PA College intellectual property may also not be used in connection with any online conduct.

Asset and Proprietary Information Security

Faculty, staff, students, and trusted third parties have the following responsibilities to uphold when working with PA College accounts, networks, and systems:

- All mobile and computing devices that connect to the internal network or access PA College data/information or other PA College resources must comply with the *Security of Data and Information Policy* as well as with the *Security of Data and Information Standards*.
- System default accounts and passwords/passphrases must be changed/removed once implemented.
- Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Policy Compliance

I. Compliance Measurement
   a. The Department of Information Technology Services team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

II. Exceptions
   a. Any exception to the policy must be approved by the PA College Department of Information Technology Services team in advance. An exception can be requested through the service request form.

III. Non-Compliance
   a. Where there is evidence of violation of this policy, PA College may restrict or prohibit the use of its information communication technology resources. Violations of this policy shall be treated in accordance with applicable College policies and procedures. When a potential violation is identified, the appropriate department head, Department of Information Technology Services, and any other PA College employees or agents as are deemed appropriate, are authorized to investigate and initiate action in accordance with PA College policy. Violations may result in suspension or termination of service(s). In addition, PA College may require restitution for any use of information systems that

violates this policy. PA College may also provide evidence of possible illegal or criminal activity to law enforcement authorities.

References: Security of Data and Information Policy; Security of Data and Information Standards; Privacy of Data and Information Policy

Audience:	All College
Effective Date:	6/1/15
Date Revised:	3/28/19
Date Reviewed:	3/28/19
Owner:	AVP IT