ALBANY COLLEGE OF PHARMACY
AND HEALTH SCIENCES

ALBANY COLLEGE OF PHARMACY AND HEALTH SCIENCES
COMPUTER USE AND COMPUTING ETHICS POLICY

(available on pp. 70-74 of 2017-18 Student Handbook)

Users of computer systems and networks at the Albany College of Pharmacy and Health Sciences must read, understand, and agree to comply with the Albany College of Pharmacy and Health Sciences Computing Ethics Policy. This policy applies to all members of the College Community (students, faculty and staff). These resources are vital for the fulfillment of the academic, research and business needs of the College community. Their use is provided as a privilege. If the Albany College of Pharmacy and Health Sciences Chief Technology Officer asks you to cease an activity on the computer, you must stop that activity immediately. Each individual faculty member, staff member, and student must exercise responsible, professional and ethical behavior when using these resources. You are responsible for your actions. That responsibility exists regardless of what security mechanisms are in place.

Access to the system is a privilege, not a right.

It is your responsibility to promptly report any violation of this policy or other College code, policy or guideline. In addition, you must report any information relating to a flaw in or bypass of resource security to the system administrator

Upon notification of a claim that any material resident on the system infringes a copyright or other intellectual property right the College reserves the right to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

The College reserves the right to remove, or disable access to material, which in the College's determination, contains defamatory, obscene, or pornographic material or otherwise violates any provisions of this policy, or adversely affects the mission of the College.

Illegal activities may be reported to local, state or federal authorities, as appropriate, for investigation and prosecution.

Privacy

While the College desires to maintain user privacy and to avoid the unnecessary interruption of user activities, the College reserves the right to investigate use of College resources, which may include the inspection of data stored or transmitted on the network including data that you have protected with a password or otherwise. By attaching a personal computer to the network (wired or wireless) you authorize and consent that the College examine the content of that computer or of any files or materials stored by you on the network. You should not consider any computer activity or any stored content, whether on your computer or on the network to be private as the Albany College of Pharmacy and Health Sciences has the unconditional right to monitor the computer system and to examine user files including Internet and e-mail usage.

Remember the Internet is not secure. If you are going to transmit sensitive data or files across the Internet you must take precautions to protect it from unauthorized access. Data and files can easily be intercepted and read, altered, misused or destroyed. In addition, machines attached to Internet are vulnerable. Do not assume your data is safe on your computer if it is directly connected to Internet. Do not store valuable or privileged information on these systems without applying security. If you can't afford to lose it, back it up.

Your password is the only means you have of keeping your account and files secure from unauthorized access. It is possible for your password to be stolen when using the Internet so you are encouraged to change it often.

Do not consider e-mail private or secure.

ACPHS Security

ACPHS information security best practices are those steps that the College and you can take on your own to help secure the computing resources that you use. Best Practices are a combination of information security tips, tools, and techniques that you can use to protect your resources and data.

Mobile computing devices are devices such as tablets, smart phones, e-readers, and laptop computers. The very features that make these devices useful (portability, access connectivity, data storage, processing power) also make them a security risk to users and to ACPHS when they contain College data. Major features of mobile devices that cause a risk to the user and potentially the College include their small size (they can be easily lost, stolen, or misplaced); weak user authentication mechanisms that can be easily compromised or simply disabled by the user; and their ease of interconnectedness.

As mobile devices become more powerful and ubiquitous, they need to be treated with the same or greater care than personal computers. This document explains general end-user security measures that can be taken on mobile devices. Taking action to personally ensure computer security helps protect everyone from data and identity theft, viruses, hackers, and other threats. Every member of the ACPHS community who uses a computing device makes ACPHS's computing environment more secure by following these best practices.

Mobile devices purchased by the College and personally owned Mobile devices connected to or accessing ACPHS' password protected network (hereafter covered mobile devices) must comply with the following:

Mandatory compliance requires:

1. Compliance with the ACPHS HIPAA Security Policy in accordance with the HITECH statute and implementing regulations.
2. Security software to be installed on covered mobile devices prior to deployment. If a device is already deployed, and it doesn't have the security software, IT must be contacted to install the software on the device. It violates the College's security policy of the security software is uninstalled by the end user.

3. Covered mobile devices must be password protected and auto lock enabled. Disable Simple Passcode to allow the use of longer, alphanumeric, passcodes.
4. Covered mobile devices must be encrypted.
   a. Android - need to turn on the encryption.
   b. Windows 8 Phones – need to turn on encryption.
   c. Blackberry devices require you to turn on data protection.
   d. iPhone has built in hardware encryption but you need to turn on the password feature in order for it to be functional.
5. Enable a “remote wipe” feature if available. This also includes features that delete data stored on the mobile device if a password is not entered correctly after a certain number of specified tries.
6. Jailbreaking is the process of removing the limitations on devices installed by the manufacturer. Jailbreaking permits root access to the operating system, allowing the download of additional applications, extensions, and themes that are unavailable through the official source. You may not circumvent security features or otherwise “jailbreak” your mobile device
7. Before disposing of a covered mobile device the IT department must securely delete the data.
8. The IT department needs to be contacted if a mobile device is lost, stolen or misplaced so it can be remotely wiped.

General Security Best Practices

- Keep your mobile devices with you at all times or store them in a secured location when not in use. Do not leave your mobile devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).
- Standard security protocols should be followed. This includes ensuring your device has current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled if possible.
- Lost, stolen, or misplaced mobile devices should be immediately reported to the police. If your mobile device contained ACPHS data, also inform the ITS department about a lost, stolen, or misplaced device.

Transmission Security

- Where possible, data transmissions from mobile devices should be encrypted.
- Wireless access, such as Bluetooth, Wi-Fi, etc., to the mobile device should be disabled when not in use to prevent unauthorized wireless access to the device.

  In general, keep your wireless connection on hidden mode unless you specifically need to be visible to others.

- If available wireless access should be configured to query the user for confirmation before connecting to wireless networks.

For example, when Bluetooth is on, select the “check with me before connecting” option to prevent automatic connections with other devices.

Application and Data Security

- Do not install software from unknown sources as they may include software harmful to your device. Research the software that you intend to install to make sure that it is legitimate.
- When installing software, review the application permissions. Modern applications may share more information about you than you are comfortable with, including allowing for real time tracking of your location.
- Be careful when storing your personal data on your mobile device. If you lose the device, you could lose your data.

Use of System Resources - Dos

You must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of your account by unauthorized persons. You must not share your password with anyone else or provide access to ACPHS network resources to unauthorized persons.

Individuals who are authorized to access sensitive or institutional data are prohibited from divulging that data to any other individual, unless that individual is also authorized to use the data. Individuals are only permitted to access data as authorized. Even if a file is readable, do not assume you may read it unless explicitly granted authority to do so. Even if a file is updatable, do not modify it unless explicitly granted authority to do so

Keep all valuable digital media in a secure place. When throwing out digital media make sure no sensitive information can be found on them.

The College is not responsible for information, including photographic images and musical recordings, published on or accessible through personal web pages, including personal home pages. The College does not monitor the contents of these personal web pages. The individual or group creating or maintaining personal web pages is solely responsible for the content of the web page and may be held civilly and criminally liable for the materials posted on the web site. The College reserves the right to remove, or disable access to any material stored on any College Resources or connected to College resources.

Use of System Resources - Don’ts

You may not use College resources for your own commercial gain, or to operate or support a non-College related business or charity, or for other commercial or charitable purposes not officially approved by the College’s President.

You may not use College resources in a manner inconsistent with the College's contractual obligations to suppliers of those resources or with any published College policy.

You may not use College resources in a manner inconsistent with the norms of professional performance and conduct appropriate to your position with the College.

Game playing is not allowed on computers owned by the College. Game playing is allowed on student computers as long as it does not deteriorate system performance.

You may not move or take any hardware without explicit permission from the designated owner of that hardware.
You may not destroy or vandalize any hardware, cable or service provided by the campus. You may not authorize or allow another person or organization to use your computer accounts or ACPHS network resources.

The following are considered unacceptable uses of computer systems, and are strictly prohibited:

- Causing personal or emotional injury including: harassment or threats to specific individuals, or a class of individuals; transmitting unsolicited information that contains obscene, pornographic indecent, lewd or lascivious material or other material which explicitly or implicitly refers to sexual conduct; using e-mail or newsgroups to threaten or stalk someone; transmitting unsolicited information that contains profane language or panders to bigotry, sexism, or other forms of prohibited discrimination.
- Computer fraud.
- Computer invasion of privacy - unauthorized examination of files.
- Damage or impairment of College resources or the resources of others. Use of any resource irresponsibly or in a manner that adversely affects the work of others. This includes intentionally, recklessly or negligently (1) damaging any system (e.g., by the introduction of any so-called "virus", "worm", or "trojan-horse" program), (2) damaging or violating the privacy of information not belonging to you, or (3) misusing or allowing misuse of system resources including use of College resources for non-College related activities that unduly increase network load (e.g., chain mail, network games and spamming). Causing denial of computer services (i.e.: run a virus that renders a network unusable). Preventing others from using computer services
- Interference or impairment to the activities of others, including creating, modifying, executing or retransmitting any computer program or instructions intended to (1) obscure the true identity of the sender of electronic mail or electronic messages, such as the forgery of electronic mail or the alteration of system or user data used to identify the sender of electronic e-mail, (2) bypass, subvert, or otherwise render ineffective the security or access control measures on any network or computer system without the permission of the owner, or (3) examine or collect data from the network (e.g., a
"network sniffer" program).
- Unauthorized access and use of the resources of others, including use of: College resources to gain unauthorized access to resources of this or other institutions, organizations, or individuals; providing false or misleading information for the purpose of obtaining access to unauthorized resources; accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system or file; modification or destruction of programs or data other than your own personal files.

- Unauthorized transfer of software or data. The Internet is a global network, and the importing and exporting of software may fall under the jurisdiction of the United States Department of Commerce. Exporting can occur when hardware or software is provided to persons or entities outside the United States, and may require a license. The exportation of networking code or encryption code is restricted. You may not allow access to a restricted machine to persons or entities outside of the United States. Please be aware when posting information to a bulletin board, that data will probably cross the border. If you have any questions on the legality of transmissions over the borders of the United States, please seek legal counsel.

- Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose, including: use of system resources to commit a crime (embezzlement, harassment, blackmail etc.); theft of computer related materials; theft of computer services(for example you may not use any pay service without paying); cracking passwords

- Violating copyrights and other intellectual property rights. Whenever you are shipping software from one place to another, you must consider intellectual property and license issues. You should assume all software, graphic images, music, and the like are copyrighted. Copying or downloading copyrighted materials without the authorization of the copyright owner is against the law, and may result in civil and criminal penalties, including fines and imprisonment.

The College reserves the right to remove from the network and/or from any web page hosted on the network, any material which is not related to the work of the individual or to research being conducted by the individual which in the College's reasonable belief adversely affects the mission of the College.

VIOLATION OF THESE POLICIES MAY LEAD TO SUSPENSION OR LOSS OF PRIVILEGE, AND MAY LEAD TO EXPULSION OR TERMINATION OF EMPLOYMENT

Reports of unauthorized use or misuse of the resources will be investigated. In the event that use is determined to be contrary to College policy or applicable law, appropriate measures will be taken. These measures may include, but are not limited to, permanent or temporary suspension of user privileges, deletion of files, disconnection from the ACPHS network, referral to student or employee disciplinary processes, expulsion or termination of employment.