Massachusetts College of Pharmacy and Health Sciences
Information Services Acceptable Use Policy

Due to the ever-increasing need for integrated technology and data sharing, and because of legal and ethical requirements, all members of the College community need to be aware of their responsibilities related to data and computing at all College facilities.

I. Purpose:

This document describes the policies and guidelines for the use of the College's computer resources and use of College-wide data. Use of College-owned computers, network resources, and file-server space is a privilege extended by Massachusetts College of Pharmacy and Health Sciences to students, employees, and other authorized users as a tool to promote academic and administrative purposes. Any activity that is not listed here, which violates local, state or federal laws is considered a violation of the Massachusetts College of Pharmacy and Health Sciences Acceptable Use Policy.

II. Scope:

This policy applies to all technology users accessing resources within the Massachusetts College of Pharmacy and Health Sciences network, either remotely or via on-campus equipment. All faculty, staff, and students are expected to adhere to this policy. This policy also extends to any individual or group who accesses data, network bandwidth, or other College-owned technology equipment. Individuals who have been provided access to MCPHS' electronic resources are responsible to maintain security of all information that is stored on each system.

III. General Policies:

All users of MCPHS technology resources are required to follow these general computing guidelines. Misuse of computer resources, including but not limited to these guidelines, may result in the termination of the individual's computer account(s), revocation of computer lab access, and/or other disciplinary or legal action as deemed appropriate.

Account Use:

1. All users are responsible for maintaining the security of all account information used to access MCPHS networks and resources.

    a. Authorized users are not allowed to share accounts with others. The authorized user is responsible for all activity associated with the account.
    b. Passwords must be changed often, and never revealed to others. Strict complexity requirements have been implemented, and all accounts that access network resources must follow these requirements.
    c. The MCPHS Information Services Department does not have access to user passwords. All password requests must be accompanied by presentation of a student or faculty/staff identification card, or other form of photo ID or verbal confirmation of information.
    d. Authorized users must log out of their accounts when finished. "Locked" workstations in public areas are not permitted. Data loss, due to a restart to "unlock" a workstation, is at the risk of the account owner.
    e. All members of the MCPHS community need to be aware of virus threats, and work in conjunction with Information Services to ensure that propagations do not occur on MCPHS equipment or systems.

2. Users may not use an MCPHS account to represent anyone other than themselves, and may not use an MCPHS account that they are not authorized to use. They may not knowingly or unknowingly use an MCPHS account to access any resource for which they have not obtained appropriate approval.

3. All users are responsible for maintaining their allotted file space, and are not permitted to utilize network or file server disk space with unnecessary files (i.e. music files, non-College related pictures, movies, etc.). Information Services reserves the right to periodically scan server storage for unauthorized files and take steps to remove them.

4. Sexually explicit content, such as movies or pictures, is strictly prohibited on the College's network. Any member of the College community found to be in possession of inappropriate content will be reported to the appropriate Dean and/or Human Resources.

5. Users are responsible for archiving their files while authority is granted to access the MCPHS network resources. Accounts will be deleted when employment is terminated; student status ends in situations other than graduation, or at the discretion of the College. Information Services is under no obligation to recover or protect files from deleted accounts.

Software Use:

1. Users must follow the copyright laws, trademark standards, software license agreements, and patent information governing software that they use.

    a. Copying software is generally illegal.
    b. The College will support copying exceptions only when authorized in writing by the software publisher.

2. To determine the copyright policies for College-owned software, users should contact the Help Desk for assistance. In addition, please refer to the Library's guide sheet on Copyright and Using e-Resources, which can be found at https://my.mcphs.edu/Library/ForFaculty/copright.aspx.

Network Use:

1. Access to the Internet and the College network is managed by MCPHS Information Services.

2. Any transmission of data (i.e. email, internet files, web pages, printed files, etc.) is governed by these guidelines.

3. Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

    a. Copyrighted material
    b. Material protected by trade secrets
    c. Illegal activities (i.e. file sharing, SPAM generation, etc.)

4. Transmission of non-College related data is prohibited. Exceptions may be authorized with approval by Information Services. This includes, but is not limited to:

    a. Product advertising (outside of College-sponsored organizations, etc.)
    b. Political lobbying or religious material (outside of College-sponsored organizations, etc.)
    c. For-profit work (e.g. home businesses, etc.)
    d. Promoting external organizations (except when College-approved)

5. Content and activity on the College network is not private. Information Services technicians and administrators may monitor activity on the network as a result of their job functions and at the request of authorized individuals.

6. MCPHS Information Services will not actively monitor content of information transmitted over the network, but will investigate any/all complaints of possible misuse or inappropriate content. In the course of investigating complaints, MCPHS Information Services staff will attempt to safeguard the privacy of all involved parties.

Security Information:

1) Individuals who have been provided access to MCPHS' electronic resources are responsible to maintain security of all information that is stored on each system.
2) All members of the MCPHS community may only access resources for which they have been approved.
3) All system passwords, account names, PINs (Personal Identification Numbers) and any other type of identifying security information must be maintained, protected and never inappropriately shared.
4) All members of the MCPHS community need to be aware of virus threats, and work in conjunction with Information Services to ensure that propagations do not occur on MCPHS equipment or systems.
5) MCPHS equipment should only be used for endeavors that further the mission of the College; however limited incidental personal use may be appropriate.
6) Downloading of software, files, music, movies, etc. is prohibited when resulting in copyright infringement or excessive bandwidth usage. (Please see MCPHS Information Services File Sharing Policy for further clarification)
7) Each individual is responsible for knowing his/her departmental expectations for use of the College's equipment and systems. No member of the MCPHS community may conduct outside "business" transactions utilizing the College's equipment and systems.

Personal Hardware:

1. All personal equipment that is attached to College-owned equipment, including the network, may be subject to access while the College is performing maintenance, monitoring, or other activities. This may include:
   - Blackberry Wireless Communicators
   - Smart Phones and other hand held devices with PC-Sync technology
   - Digital cameras and camcorders
   - Laptops, iPads or other tablet and e-reader devices purchased by the individual

2. MCPHS Information Services is not responsible for repair or replacement of non-MCPHS equipment.
3. Personal computing equipment is prohibited from connecting to the MCPHS production network environment.

Electronic Communication Use:

Electronic communications include, but are not limited to: the World Wide Web, social media such as Facebook or Twitter, internet-based bulletin boards, chat groups, forums, electronic mail, and instant messaging, etc. Electronic communications are any information, graphics, or data sent or retrieved via electronic systems.

Unacceptable uses of electronic communication include, but are not limited to the following:

1. Conducting unlawful activities
2. Use for any commercial activities
3. Sending offensive or abusive messages
4. Use to gather or other collect information about others for commercial or private use
5. Use for fund raising, political campaign activities, or public relations activities not specifically related to MCPHS sanctioned activities
6. Use to conduct or forward illegal contests, pyramid schemes or chain letters, or to spam
7. Use to sell access to the Internet
8. Use to conduct any activity which adversely affects the availability, confidentiality or integrity of MCPHS' technology
9. Use to benefit personal or financial interests

10. Forging electronic communications
11. Intentionally transmitting computer viruses

MCPHS Information Services attempts to provide secure and reliable electronic communication services. However, secure and reliable services do not in any way guarantee the confidentiality and privacy of electronic communication. Confidentiality may be compromised by applicability of law or policy, unintended redistribution, network 'sniffing' and interception, or inadequacy of current technologies to protect against unauthorized access.

Use of Email Distribution Lists:

The MCPHS provided distribution lists must only be used to distribute official information for the College and the official groups that represent it. Examples of acceptable use include College-sponsored activities, policies, security or facility alerts, or information that relates directly to MCPHS's mission and operations. MCPHS provided distribution lists may not be used as a public forum to discuss political, personal, or religious commentary, or to lodge complaints against College employees or departments. Distribution lists should not be used for personal messages, items for sale, jokes, chain letters, pyramid schemes, virus warnings (unless issued by the Office of Information Technology), unsolicited commercial emails or any information that is of interest to only a small segment of the campus audience. Derogatory, obscene, defamatory and/or harassing communications are prohibited and will lead to disciplinary action, up to and including termination.

All users should be aware of the following:

1. You should not assume confidentiality or privacy of electronic communications. It is recommended that you do not send confidential College communications (as determined by law, policy, etc.) via electronic communications.
2. In the course of routine systems maintenance, troubleshooting and mail delivery problem resolution, technical staff may inadvertently see the content of electronic mail messages. Information Services reserves the right to search electronic communication records or transactional information for violations of law or policy.
3. Electronic communication may be subject to disclosure under law. Back-up copies may be retained for periods of time and in locations unknown to senders and recipients even if you have deleted it from your account or PC.
4. Messages can be easily forwarded without your permission to individuals or groups, even though it violates copyright law.
5. Messages can be intercepted while in transit through the network.
6. Forwarded messages can be altered from the original copy.
7. Once a message is received on a machine outside of MCPHS, all of the above concerns continue to apply.

Email Web Access

Access to Electronic Mail through Web client software is subject to the same policies and guidelines as email obtained via a desktop client.

Internet Use:

1. MCPHS assumes no responsibility for any direct or indirect damages incurred as a result of a user's connection to the Internet via College resources.
2. MCPHS is not responsible for the accuracy of information found on the Internet, and merely provides an avenue to access and distribute the information via its systems.

Personal Use of College-Owned Computer Systems:

1. College-owned computers are provided to employees to accomplish the job functions assigned at the time of hire.

2. College-owned computers are provided to students to assist with the academic functions of the College. Email is intended to be used for instructor-to-student and student-to-student communications. Internet access is provided to assist with assignments, research, etc.
3. Use of College-owned computers to play online games, unless specifically assigned as a learning tool, is strictly prohibited. This includes all internet and network versions of popular multi-player games.

System Protection and Resource Limitations

MCPHS Information Services reserves the right to:

1) Set the amount of disk space available for electronic communications mailboxes, as well as network file storage for all authorized users
    a. Student mailboxes have a 25Mb storage limit
        i. "Deleted Items" folder is emptied nightly
        ii. Messages are kept for one semester, and purged after grades are posted.
    b. Staff mailboxes currently have no storage limit, but Information Services reserves the right to amend this at any time.
        i. All messages over 180 days will be sent to the "Deleted Items" folder
2) Carry out necessary purges of information stored on the servers to preserve the integrity of the system
3) Run virus scans and quarantine electronic communications that contain viruses

Users are responsible for retaining their own records and therefore are advised to keep back-up copies of important documents, distribution lists, and calendars on appropriate backup media.

Security

MCPHS Information Services attempts to provide secure and reliable electronic communication services. However, secure and reliable services do not in any way guarantee the confidentiality and privacy of electronic communication, which is the electronic equivalent of sending a postcard. Confidentiality may be compromised by applicability of law or policy, unintended redistribution, network 'sniffing' and interception, or inadequacy of current technologies to protect against unauthorized access.

Password Complexity Requirements:

All domain passwords (which allow access to file servers, printing resources, email accounts, proxy access, as well as WebAdvisor, and Blackboard learning resources) must meet the following complexity requirements:

- Password must be at least 8 characters long
- Password must contain at least 3 of the following: uppercase letter, lowercase letter, number or symbol
- Password cannot contain any part of the username or student ID number
- Passwords cannot be "recycled" or used more than once. Passwords must be **UNIQUE** combinations using the requirements above.
- Passwords must be changed every 90 days, equaling 4 times per calendar year.

When your password's expiration date is drawing near, you will begin to receive notification in the form of a visible prompt on your screen, if you are on a College-owned PC. You will have 14 days to comply with the request. If you are predominately off campus, it is recommended that you set a personal calendar reminder to change your password every 90 days (or more frequently). If you fail to change your password during the

14 day grace period, your password will expire and your access to MCPHS systems will be revoked until you contact Information Services.

File Sharing/Peer-to-Peer Usage:

File-sharing and the use of Peer-to-Peer (P2P) programs have become increasingly popular in academic environments. Unfortunately, the majority of instances are utilized for illegal file copying, distribution, etc. Unauthorized distribution of copyrighted materials such as music, movies and video distributed via unauthorized P2P filing sharing may result in civil and criminal penalties in addition to MCPHS discipline. Both the person who makes the copyrighted work available for download and the person who receives or downloads the unauthorized copy have violated copyright laws and MCPHS policy. In an effort to maintain a network that is stable, secure, and virus-free, the use of P2P programs is prohibited.

1. Peer-to-peer file sharing applications including: (but not limited to) Napster, Gnutella, Kazaa, AudioGalaxy, iMesh, and others, may not be installed or used on computers owned or managed by the College.
2. Peer-to-peer file sharing applications including: (but not limited to) Napster, Gnutella, Kazaa, AudioGalaxy, iMesh, and others, may not be installed or used on computers attached to the College's network, regardless of their ownership.
3. Information Services staff may, in order to ensure compliance with the College's policies and Federal or State Law, inspect and remove any of the prohibited software from any equipment currently or previously attached to the College's network.

The College blocks access to many of these file sharing packages, rendering them unusable. It is strongly recommended that they be removed immediately, prior to attaching the PC to the College network.

If an artist, author, publisher, the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), or a law enforcement agency notifies the College that a Faculty/Staff member or Student is violating copyright laws, Information Services will provide information in the form of Internet Protocol (IP) address information and any information from logs to assist in the investigation of the complaint. If appropriate, action will be taken against the violator in accordance with the College's policy. In some cases, violations of College policy can result in suspension or revocation of network access privileges and/or civil or criminal prosecution under state and federal statutes.

Upon receiving notice from either Information Services' internal reporting system or from external sources (RIAA, MPAAMPA, or law enforcement agency), the following processes will be employed:

For Students:

1. ***For a 1st Offense:***
    1. MCPHS user is immediately denied access and notified with a written warning.
    2. The Dean of Students is contacted.
    3. Information Services receives return of the written warning with signature that the offender has acknowledged the warning and is providing signed commitment to refrain from further activity.
    4. MCPHS user is given access.
2. ***For 2nd Offense:***
    1. MCPHS user is immediately denied access and notified with a written warning.
    2. Written notice identifies that all network access is denied for one week from date of offense.
    3. The Dean of Students is provided a copy of the written notice.
3. ***For 3rd Offense:***

    The student's Internet connection will be immediately disconnected. The matter will be referred to the Student Discipline System for remedies up to and including termination of student status.

For Employees:

For any offense, failure to comply with the guidelines presented herein shall result in disciplinary action, up to and including termination of employment.

In addition to the general computing policies above, students must also be aware of the following:

Access to Computer Resources:

1. All students must have a current valid MCPHS student ID card to obtain entry to the computer labs on campus.
2. Computer labs are available on campus for all students to complete assignments, research, etc. Hours are posted, and all students are expected to follow posted rules of conduct.

Authorized Uses of College-Owned Computer Systems:

1. Students may utilize College-owned computers to complete assignments, research information, prepare resumes, and utilize online learning tools.
2. Students may not utilize College-owned computers to play online or locally installed games, promote businesses, or otherwise perform non-academic functions.
3. Using non-approved print media (i.e. transparencies, etc.) is prohibited.
4. Students are not authorized to install or remove any applications from College-owned computers.

    a. A class instructor who identifies a need to install or remove a program must request exceptions prior to the start of a semester, to allow for appropriate testing and image creation.
    b. All requests for additional software must be submitted to MCPHS Information Services no less than 2 weeks in advance of a semester's start date.