Westchester Community College Student Technology Use Policy

Version 1 / Sept 22, 2009

Table of Contents

1. Introduction

Information and information systems are key assets of Westchester Community College ("the College"). Technology has become an integral component of the learning process and is part of most students daily education. The College provides systems, including the computers, networks, technology applications and the information housed therein to permit students access to information and applications they need to further their education.

This policy sets forth a basic set of standards for use and protection of computer and information assets. It includes but is not limited to computer workstations, laptop computers, networks and connection(s) to the Intranet, Internet and any other information technology services available both now and in the future.

This policy covers all students of the College. It also covers any other individuals who have access to College technology facilities, computers or networks.

Inappropriate use of equipment and services exposes the College to risks including virus attacks, system compromise, interruption of services and litigation.

It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

2. Prohibited Use

Improper uses of College Systems include, but are not limited to:

2.1. Misrepresenting, obscuring, suppressing or replacing any identity on an electronic communication;
2.2. Any use or communication in violation of other College policies;
2.3. Any use of profanity, obscenities, or suggestive, intimidating, hostile, discriminatory or derogatory remarks, even in jest;
2.4. Downloading of copyrighted material;
2.5. Using college systems in any outside business activity;
2.6. Gambling;
2.7. Any test or attempt to compromise computer or communication system security;
2.8. Any use that violates federal, state, or local law or regulation;
2.9. Knowingly or recklessly disrupting the normal operation of computers, peripherals, or networks. "Disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service and forged routing information for malicious purposes;
2.10. Connecting unauthorized equipment to the network for any purpose;
2.11. Running or installing games or any other unauthorized software on College computers, including personal Web servers;
2.12. Copying of any software from College computers;
2.13. Using the College network to gain unauthorized access to any computer system;
2.14. Using College systems to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist, violent, drug-related or other offensive material (including messages, images, video, or sound) unless expressly required for educational purposes;
2.15. Using College systems in such a way as to create an intimidating or hostile environment;

2.16. Using College systems to solicit for personal gain or for the advancement of a political or religious belief;
2.17. Modifying College-issued computer software, especially anti-virus / security software.

3. Monitoring & Privacy of Communications

The College maintains the right to access and examine College computer systems and networks and all information that is stored or transmitted through these systems and networks, including all e-mail and website visits.

4. Identification and Passwords (PeopleSoft)

Each College student must be positively identified prior to being able to use any on-line College resource.

Each person is responsible for all activity that occurs on his or her User-ID. Whenever a student walks away from their computer they should logout so no unauthorized person can access their personal information.

The password policy applies to all users who sign on to College resources. The policy is meant to eliminate the use of `weak' passwords which can be easily guessed and which are often the cause of data theft or malicious attacks on networks.

The rules for passwords changed are as follows:

- Must be at least 7 characters long;
- The password contains characters from all three of the following categories:
  - Uppercase characters (A - Z)
  - Lowercase characters (a - z)
  - Base 10 digits (0 – 9)
- Symbols found on the keyboard are also allowed but not required (all keyboard characters not defined as letters or numerals):'_!@#$%^&*O_+-={}ILI~=";'<>`?,./
- An old password cannot be re-used. A history of your previous passwords is maintained to ensure they cannot be re-used.

These complexity requirements are enforced when passwords are initially created and changed.

It is the responsibility of each student to protect the confidentiality of his/her password. Passwords must not be shared with others nor recorded in any place where they might be found.

5. Use of Outside Technology

All non-College PCs, laptops, MACs, and other computing equipment are permitted to connected to the College's wireless network and wired jacks at designated locations in the Library, these devices are banned from connecting to the College wired network.

As a convenience to students and visitors, the College provides Internet access through wireless access points, known as the Asgard wireless network, throughout campus. When you attach to the Internet using these facilities, we strongly recommend that you protect yourself against other users by practicing safe computing. This means that at a minimum, you should have:

1. Up-to-date virus protection
2. All Windows/MAC security patches installed

In no case is Westchester Community College responsible for data loss resulting from the use of the wireless access points or student-accessible connections.

6. Computer Software

The installation of software on College owned computers is the responsibility of the IT Department. Students are not permitted to install software under any circumstance.

7. Software Licensing/Copyright Agreements

The duplication of copyrighted material is a violation of the federal copyright law and may result in civil and criminal penalties, and disciplinary action by the College. Under federal copyright law, software may not be duplicated for any reason except those stated in the software license agreement. The College prohibits the duplication and sharing of any copyrighted material (software, video, audio) using any electronic means, including peer-to-peer applications.

Westchester Community College licenses the use of its computer software from a variety of outside companies. Westchester Community College does not own this software or its related documentation and unless authorized by the software developer in writing, does not have the right to reproduce it.

When enrolling at Westchester Community College, students are granted use of the College's computer facilities for educational purposes only. Students are not permitted to use peer-to-peer applications or perform any activities using college computer equipment that would violate any federal or state laws, including but not limited to, for the duplication and/or distribution of copyrighted material.

Because of federal and state laws and the penalties they impose, Westchester Community College students making, acquiring or using unauthorized copies of copyrighted material are in violation of federal and state copyright laws and could be subject to disciplinary actions, including academic dismissal from the College in addition to possible penalties under the law. Possible penalties for copyright infringement include fines and imprisonment.

For your information, particularly with regard to penalties, violators of the Digital Millennium Copyright Act who illegally shared copyrighted files are subject to civil penalties of between $750 and $150,000 per song. In the past, pre-litigation settlements offered by copyright owners have ranged from $3,000 to $4,000 and up. Additionally, a court may, in its discretion, grant the

copyright owner reasonable attorney fees. Although prosecution of students for this type of file sharing is extremely rare, 17 USC § 506 lays out criminal penalties for intentional copyright infringement which can include fines and jail time.

For more information regarding acceptable uses of copyrighted material, please visit http://www.sunywcc.edu/library/research/copyright.htm.

Appendix A: Computer & Communications Technology Use Policy

A. Purpose

Westchester Community College owns and operates a variety of computing systems which are provided for the use of Westchester Community College students, faculty and staff in support of the programs of the college and are to be used for education, research, academic development and administrative purposes only. Commercial uses are specifically excluded. All students, faculty, and staff are responsible for seeing that these computing facilities are used in an effective, efficient, ethical and lawful manner. This document establishes rules and prohibitions that define acceptable use of these systems. Fraudulent, harassing, pornographic or obscene messages and/or materials are not to be accessed, sent or stored. Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as discipline or legal sanctions under Federal, State and local laws and Westchester Community College policies.

B. Audience & Agreement

All users of Westchester Community College computing systems must read, understand and comply with the policies outlined in this document as well as any additional guidelines established by the administrators of each system or facility. Such guidelines will be reviewed by the appropriate college governance bodies. BY USING ANY OF THESE SYSTEMS, USERS AGREE THAT THEY WILL COMPLY WITH THESE POLICIES.

C. Rights

These computer systems, facilities and accounts are owned and operated by Westchester Community College. Westchester Community College reserves all rights, including termination of service without notice, to the computing resources which it owns and operates. These procedures shall not be construed as a waiver of any rights of Westchester Community College, nor shall they conflict with applicable law. Users have rights that may be protected by Federal, State and local laws.

D. Privileges

Access and privileges on Westchester Community College computing systems are assigned and managed by the administrators of specific individual systems and facilities. Administrators, faculty, staff and students may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system. Users may not, under any circumstances, transfer these privileges to other individuals.

E. Responsibilities

Users are responsible for maintaining the following:

i. An environment in which access to all College computing resources is shared according to system and facility policy between users. In meeting this responsibility, users may not plug any peripheral equipment, with the exception of USB memory sticks connected via front-mounted USB ports only, into any computer owned by Westchester Community College. This includes, but is not limited to: trackballs, printers, portable hard drives, and game controllers.

ii. An environment conducive to learning: A user, who uses the college's computing systems to harass, or make defamatory remarks, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks shall bear sole responsibility for their actions. Users agree that Westchester Community College's role in managing these systems is only as an information carrier, and transmission through these systems will never be considered an endorsement by Westchester Community College.

iii. An environment free of illegal or malicious acts: The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which (s)he is authorized, or any attempt to deprive other authorized users of resources or access to any Westchester Community College computer system shall be regarded as malicious, and may be treated as an illegal act.

Many of the Westchester Community College computing systems provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material which may be considered offensive or objectionable in nature or content. Users are further advised that Westchester Community College does not assume responsibility for the contents of any of these outside networks. The users agree to comply with the acceptable use guidelines and proper etiquette for whichever outside networks or services they may access through Westchester Community College systems. The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service). The user agrees that, if someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not Westchester Community College, which is acting solely as the information carrier.

iv. A secure environment: Any user who finds a possible security lapse on any system is obliged to report it to the system administrators.

Knowledge of passwords or loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given. Users are responsible for backup of their own data, except for data saved on the network.

F. Accounts

All accounts assigned to an individual must not be used by others. The individual is responsible for the proper use of the account, including proper password protection.

G. Confidentiality

Programs and files are confidential unless they have been made available, with written permission, to other authorized individuals. When performing maintenance, every effort is made to insure the privacy of a user's files. If policy violations are discovered, they will be reported immediately to the appropriate system administrator.

H. System Performance

No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any college computer system.

I. Copyright

Computer software protected by copyright is not to be copied except as permitted by law, or by the contract with the owner of the copyright. Illegal copying of copyrighted software is a felony offense under New York State and Federal law.

J. Peer-to Peer Software

To help prevent copyright violations, use of Peer to Peer (P2P), often called file sharing software, is prohibited on college computers and the college network. This prohibition also minimizes the risk to college computers and the network from unwanted software and excessive bandwidth use. It is a felony offense to download and/or share any copyrighted materials.

K. Violations

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violation will be confidentially reported to the appropriate system administrator. Violations of these policies will be dealt with in the same manner as violations of other college policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the college and legal action. Violations of some of the above, policies may constitute a criminal offense.

L. Additional Guidelines

System and facility administrators will establish more detailed guidelines, as needed, for specific computer facilities.