

Westchester Community College Technology Use Policy

Version 1 / Feb 19, 2009

Table of Contents

Introduction.....	3
Ownership	3
Personal Use.....	3
Prohibited Use.....	4
Blogging	4
Monitoring & Privacy of Communications	5
PC Software Auditing.....	6
Identification and Passwords.....	6
Unauthorized Access	7
Remote Access.....	7
USB Sticks & Mass Storage Devices	8
Use of Outside Technology.....	8
Technology Inventory	8
PC Software	8
Computer Virus Protection	9
E-mail & Communications Activities	9
Physical Security.....	10
Preventing Identity Theft	10
Software Licensing/Copyright Agreements.....	11
Responsibilities.....	11
 Appendixes	
Appendix A (PC Auditing).....	12
Appendix B (Unauthorized Network Access)	14
Appendix C (Requesting e-mail and remote access)	15
Appendix D (Wireless Access).....	16
Appendix E (Certification of Equipment).....	17
Appendix F (Saving Files to a Network Location).....	19

Appendix G (Computer & Communications Technology Use Policy)	20
Appendix J (Other Items of Interest)	23
Appendix K (Computer Supply Request)	24

1. Introduction

Information and information systems are key assets of Westchester Community College ("the College"). They are essential to the conduct of College business and are a part of most employees' daily work. The College provides systems, including the computers, networks, technology applications and the information housed therein to permit employees to perform their duties more effectively.

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, electronic mail ("e-mail"), databases, 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 employees of the College. It also covers any other individuals, including consultants, interns, temporaries and vendors, 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.

Effective security is a team effort involving the participation and support of every College employee and affiliate who deals with data and / or information systems. It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

2. Ownership

Information processing related systems, including but not limited to: computer equipment, operating system software; application software, network accounts providing e-mail, document storage, Web browsing, File Transfer Protocol, networking and intra-net hardware and software (collectively "System(s)"), are owned by or licensed by Westchester Community College. *They are intended primarily for College business purposes.*

Equipment purchased by employees will not be considered a College asset or responsibility. Devices not supported or approved by College IT will not be configured for College use. Employee procurement of devices and service must be based on the Information Technology approved equipment list or receive IT approval prior to purchase, if connectivity to College systems is required.

In the event a College or approved personal device is lost or stolen, it must be reported immediately to Security as well as IT for disablement from our systems.

3. Personal Use

Incidental personal use of College Systems is permissible if the use:

- 3.1. Does not consume a significant amount of resources that could otherwise be used for business purposes;
- 3.2. Does not interfere with any employee's productivity;
- 3.3. Does not preempt any business activity;

3.4. Is not contrary to any other College policies. It is the responsibility of each employee and manager to ensure that the County's technology is used properly.

4. Prohibited Use

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

- 4.1. Contributing to blogs, public forums, chat rooms or message boards except for assigned business or academic related activities (see section below - "Blogging" - for details);
- 4.2. Misrepresenting, obscuring, suppressing or replacing any identity on an electronic communication;
- 4.3. Any use or communication in violation of other College policies, such as Equal Employment Opportunity policy, Harassment policies, etc;
- 4.4. Any use of profanity, obscenities, or suggestive, intimidating, hostile, discriminatory or derogatory remarks, even in jest;
- 4.5. Downloading of copyrighted material without specific permission of copyright owner;
- 4.6. Downloading of large files or data for personal use, including video, music, photographs, etc.;
- 4.7. The automated forwarding of messages outside of the College;
- 4.8. Using college systems in any outside business activity;
- 4.9. Gambling;
- 4.10. Any test or attempt to compromise computer or communication system security;
- 4.11. Any use that violates federal, state, or local law or regulation;
- 4.12. 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;
- 4.13. Connecting unauthorized equipment to the network for any purpose;
- 4.14. Running or installing games or any other unauthorized software on College computers, including personal Web servers;
- 4.15. Copying of any software from College computers, for other than archiving purposes;
- 4.16. Using the College network to gain unauthorized access to any computer system;
- 4.17. 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;
- 4.18. Using College systems in such a way as to create an intimidating or hostile work environment;
- 4.19. Using College systems to solicit for personal gain or for the advancement of a political or religious belief;
- 4.20. Modifying College-issued computer software, especially anti-virus / security software.

5. Blogging

Blogging by employees using the College's property is subject to the terms and restrictions set forth in this policy. Limited and occasional use of the College's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the College's policy, is not detrimental to the College's best interests, and does not interfere with an employee's regular work

duties. As with the use of any College computer system, blogging from the College's systems could be subject to monitoring.

Employees shall not use College property to engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the College and/or any of its employees. Employees are also prohibited from using College property to make any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the College's Non-Discrimination and Anti-Harassment policy.

In addition, employees may not use College property to attribute personal statements, opinions or beliefs regarding the College when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the College. Employees assume any and all risk associated with blogging.

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

6. 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. All electronic communications are considered College records. As College records, electronic communications are subject to disclosure to law enforcement or government officials or to other third parties through FOIL (Freedom of Information Law) requests or other process. Employees must ensure that information contained in electronic communications is accurate, appropriate and lawful.

While Westchester Community College does not intend to regularly review employees' e-mail records, employees have no right or expectation of privacy in e-mail. Since the College is responsible for the servicing and protecting of its electronic communications networks and administering this policy, it is occasionally necessary to intercept or disclose electronic communication. Access to an employee's electronic documents will be granted at the written request of their supervisor and the approval of the appropriate Cabinet member, at a cabinet member's request, or when legally required. Even though all material created on College equipment is legally the property of Westchester Community College, we only provided access to an employee's files with appropriate need and justification. This adds another layer of checks and balances to insure that access isn't provided to another individual inappropriately.

Upon an employee's termination the employee's manager may request his/her e-mail be directed to another employee to be managed.

Communications on these Systems are not private. Users should be aware that the data they create on the System remains the property of the College, and usually can be recovered even though deleted by the user. Despite security precautions, there is no absolutely fail-safe way to prevent an unauthorized user from accessing stored files. Furthermore, information that is stored on the System or sent via e-

mail may be subject to disclosure pursuant to the New York State Freedom of Information Law.

7. PC Software Auditing

Information Technology has been charged with the responsibility of enforcing copyright compliance at the College. This requires taking either physical or electronic inventory of all installed PC software on student, faculty, staff, and administrative PCs periodically on a scheduled and unannounced basis.

The audit is performed electronically with software designed to identify all computer programs and copyrighted materials installed on each PC's hard disk. The list of software will be matched to Information Technology's' inventory records. This audit may be completed on-site or over the network from a remote location.

For more details concerning the auditing process, refer to Appendix A.

8. Identification and Passwords

Each College employee must be positively identified prior to being able to use any College computer or communications system resource. Positive identification for internal College networks involves a User-ID and a password, both of which is unique to an individual and will be supplied after completion of Network Service Request form. The form can be access via http://starweb.sunywcc.edu/forms/Network_Services_Request.htm .

Each person is responsible for all activity that occurs on his or her User-ID. User-ID's will be revoked if the employee is terminated. Whenever a person walks away from their PC the employee should lock their PC so no unauthorized person can access the computer and associated applications. Each person must log off from all User-ID accounts before leaving at the end of their workday.

The password policy applies to all users who sign on to College PC's, use College e-mail, and/or access College shared file resources ("Shares"). 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 _ + - = { } | L I ~ = " ; ' < > ` ? , . /
- 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. For security purposes you are forced to change your password every 60 days. The College also enforces a password lockout policy. Your User Account will be locked after 4 failed logon attempts within 15

minutes. Your user account will be automatically unlocked after 15 minutes.

It is the responsibility of each employee 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. IT must be informed of any actual or suspected password disclosures and will reset the password accordingly.

9. Unauthorized Access

Allowing another individual to access your computer while it is still signed on to your account provides unauthorized network access to the individual and is expressly prohibited. Depending on access rights and privileges extended to the person whose sign-in is used, the unauthorized individual could access employee and/or student social security numbers and other private information, confidential college data and emails, and proprietary information. Further, such access would allow for the theft and/or destruction of such information.

This type of unauthorized access can be easily prevented. Every person is responsible for keeping either workstation secure, you should lock your workstation whenever you leave it, even if you will only be gone for a few minutes. Your workstation screensaver should also have its password protection configured to begin after a short period of inactivity (10 minutes at most is recommended). It is very easy to get sidetracked and stay away from your desk longer than you anticipate, so it is best just to secure your workstation whenever you leave it.

Locking your desktop does not affect any of your running applications. To unlock your workstation, enter your network password and your desktop will return to exactly where it was prior to locking.

Locking your Workstation Manually

1. Press the Windows key (between CTRL and ALT) + the “L” key.

Setup your Workstation to lock with a password automatically

1. Right-click on the desktop.
2. Click Properties then the Screen Saver Tab.
3. Change Wait time to 10 minutes or less.
4. Select On resume, password protect.
5. Click OK.

For more details concerning the network policy, refer to Appendix B.

10. Remote Access

IT provides VPN access to the College network to facilitate effective work while away from College premises. Access is provided by IT only upon request and with appropriate cabinet level approval. VPN access for Faculty, Adjunct Faculty and Non-represented Management has been preapproved by the cabinet. VPN access to College systems is intended for College business purposes only. Use of remote access is subject to this policy and additional procedures.

Access to the College's web-based e-mail services, from <https://sunywccmail.sunywcc.edu>, is subject to the same policies covered in this document. Passwords used for these services must also be handled accordingly and must not be stored in your local computer. In addition, remote access to the College's web-based services, using non-College equipment such as kiosks or computers located in hotel business centers and local libraries must be terminated before leaving the devices.

For more details concerning the remote access policy, refer to Appendix C.

11. USB Sticks & Mass Storage Devices

An increasing number of College employees transport information on USB sticks between work and home. Although these devices are designed to be harmless, they do pose security risks for the organization. It is too easy to use them to siphon off confidential data. Even legitimate users can simply lose the device, or have it stolen. Do not store sensitive or confidential information on unencrypted USB sticks or other portable storage devices.

12. Use of Outside Technology

All PCs, laptops, and other computing equipment are banned from connecting to the College data network unless such equipment was purchased through Information Technology (IT) or prior written approval for connectivity has been granted by IT. Full time faculty, adjunct faculty, guest lecturers and vendors are permitted to connect their personal laptop to the College network after the laptop is certified as virus free and all windows critical updates have been applied. This policy excludes wireless access.

As a convenience to students and visitors, the College provides Internet access through wireless access points, known as the Asgard wireless network, throughout campus and wired jacks at designated locations in the Library.

For more details concerning wireless access, refer to Appendix D.

For more details concerning the equipment certification process, refer to Appendix E.

13. Technology Inventory

In order for the IT Department to maintain an accurate inventory of computer equipment, individuals and individual departments are not permitted to move, change or modify College computing equipment on their own. The IT Department is the only authorized entity to do that work.

To have a computer or computer equipment removed or transferred the IT Department must be notified, which can be done by contacting the helpdesk at x6665.

14. PC Software

The installation of software is the responsibility of the IT Department. Users are not permitted to install software on their own except under specific circumstances. The College has the right to audit College personal computers/laptops and remove any unauthorized software.

For more details about what software users can install and the College audit policy, refer to Appendix A.

15. Computer Virus Protection

All PCs that are owned by the College and connected to the College network continually execute virus-scanning software with a current virus database.

16. E-mail & Communications Activities

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

The following e-mail and communications activities are not allowed due to associated security risks:

- 16.1 Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);
- 16.2 Any form of harassment via email whether through language, frequency, or size of messages;
- 16.3 Unauthorized use, or forging, of email header information;
- 16.4 Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies;
- 16.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type;
- 16.6 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- 16.7 Please do not use the college's email system for anything other than official college business. For example, solicitation of funds or support for outside organizations should not be made through global emails. Also, "advocacy" emails which support a particular perspective of a political issue are also not allowed. If you're not sure whether your proposed email fits into one of these categories, please check with College-Community Relations.

E-mails to large groups of people must include an option and precise instructions, for the recipient to stop receiving the e-mails, also known as opting out. A Listserve may also be used for communications to large groups but also must include an option and precise instructions for opting out.

The following are rules for College wide e-mails:

- 16.8 College-Community Relations will assist with the distribution of campus-wide email. If you have a memo, flyer, etc., that you would like to share with the campus community, please email your document to Janice Adams along with any message you'd like sent. When in doubt about whether to send a global email, contact College-Community Relations. Due to space constraints, the use of college-wide emails should be limited.

16.9 Identify Email Recipients and Content - When sending out a college-wide email, especially one with a large attachment, please add a brief description of content in the "Subject" header. Also, provide a description of your attachment in the body of your message. This will help recipients of your message to quickly determine whether they will open the attachment or move on to other messages.

16.10 Large Attachments / Graphics - Large attachments and graphics in global emails cause problems: large emails cause employees' email boxes to become immediately filled to capacity and employees can no longer send or receive messages until the large emails are deleted. Employees so affected overwhelm the IT Help Desk with calls, preventing IT from assisting other employees. Emails with large attachments and graphics slow down the network for all of us and consume substantial network storage space.

Suggestions include removing or limiting graphics, or using smaller graphics. You may also store large attachments (typically attachments with graphics or pictures in them) in a Public Folder and send an email with a link to the file. The Help Desk can assist you with this.

17. Physical Security

Employees entrusted with College computer assets, including desktops, laptops and software, must exercise due diligence at all times to prevent theft, destruction or other misuse of the assets. Portable, laptops, notebooks, Blackberries, and other transportable computers can contain sensitive College information and must be treated with the care to safe guard the equipment and information.

18. Preventing Identity Theft

In situations in which it is essential that a particular user or office be given files with full social security numbers or other confidential data, users cannot;

- Download sensitive/confidential information to a laptop or any other portable device until IT can guarantee the security of these files once they have been downloaded.
- Download sensitive/confidential information to non-College equipment.
- Copy a whole database with confidential personal information, even to a College PC or laptop. Such data should stay in the secure Data Center.

Files should be stored on the network storage provided to each individual or the storage provided to the department. Information on how to save files to network provided storage can be found in Appendix F.

Furthermore, all users are reminded that transporting sensitive data containing social security numbers and dates of birth off-campus in any form, including hard copy, is a violation of the College's data security policy.

Our students trust the College to protect their private data. We have an ethical and, in New York State, legal obligation to protect this data. This policy is intended to respond to that obligation. In addition to the matter of downloading private data and the ban on removing such data from the campus as articulated in this policy, please be sensitive to any actions or activities that could potentially compromise private data and owners' trust in us. Do not include someone's social

security number or birth date in an email, or in an unprotected file attached to an email. It is a violation of this policy. Do not send employee or student SSNs or birth dates in emails. Do not ask employees or students to send SSNs or birth dates via email. If you have a business need to share such private information, please contact the Help Desk, x6665.

19. Software Licensing/Copyright Agreements

All personal computer software installed on College equipment must comply with the appropriate licensing protocols and copyrights relevant to that software. Any duplication of copyrighted material is a violation of the federal copyright law. Under federal copyright law, software licensed by the College which is loaded on a hard disk may not be duplicated for use on any other PC. The College prohibits the duplication of any copyrighted material 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.

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

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

20. Responsibilities

All employees are responsible for complying with this policy and for immediately reporting any known or suspected violations of this policy to their immediate supervisor or College IT.

Appendix A: (PC Auditing)

Policy

Information Technology has been charged with the responsibility of enforcing copyright compliance at Westchester Community College. This requires taking either physical or electronic inventory of all installed PC software on student, faculty, staff, and administrative PCs periodically on a scheduled and unannounced basis.

Methodology

The audit is performed electronically with software designed to identify all computer programs and copyrighted materials installed on each PC's hard disk. The list of software will be matched to Information Technology's inventory records. This audit may be completed on-site or over the network from a remote location. Note: the audit software does not inspect or in any other manner manipulate or retrieve personally created files such as documents, data files, etc

Notification of a scheduled physical PC audit will be provided no later than the previous day, either by direct contact, or by message to the division/department office. The individual whose PC is scheduled to be audited is welcome to be present at the time of the audit (audit typically takes less than 5 minutes) or have another individual present in his/her absence. Most audits will occur remotely and without need for interaction from the user.

Audits will also be conducted as part of the service call procedure, and will be deemed to be announced by virtue of the service call being initiated by the user(s) of the PC in need of service.

Software on a PC that is not WCC-registered will be removed to bring the PC into compliance with the copyright law. The matter will be discussed with the "owner" of the PC to determine circumstances and to legally purchase software as needed.

Users are strictly prohibited from installing software on College computers without prior approval from Information Technology. For personally owned software to be installed on College computers the following rules must be abided by *before* the software is installed:

- ◆ For Commercial Applications: The original media (disks, CD) and license agreement must be sent to IT to be documented and entered into the inventory control system.
- ◆ For Trialware: All software installed with a trial time period must be removed from the computer once the trial period has expired. On personally assigned College laptops, this responsibility is the users. For all College owned networked PCs, IT assumes responsibility for removing trialware.
- ◆ For Shareware: All software installed that is shareware must have a copy of the license agreement forwarded to the IT department for logging. The user installing the shareware is responsible for removing it from their personally assigned College laptop if the conditions of the product are not met. IT will uninstall any software not meeting license requirements on College networked PCs.
- ◆ For Freeware: A copy of the license agreement (or the fact that there is none) must be forwarded to the IT department.

All requests must be accompanied by a Technical Services Request and a personal Software Support Waiver. Once the conditions are met, software will be scheduled for installation by IT Technical Services. On personally assigned College laptops, software can be self-installed by the user or dropped off at the Helpdesk (TEC21E) for installation by a technician.

Violation of Copyright Law

1st Offense:

- 1) Information Technology will remove the offending software and meet with the party or parties that use the PC to review the findings, the law, actions taken, and remedies: i.e., purchase of the desired software by Information Technology for the PC; if software is privately owned by the PC user, delivery of original media to Information Technology by the PC users.
- 2) Violation and actions(s) taken by Information Technology are brought to the attention of the individual's division/department head.

2nd Offense:

Matter brought to the Cabinet for further action. This action may include, but not be limited to, removal of the PC, and personnel actions as deemed appropriate.

Appendix B: (Unauthorized Network Access)

It is important to be aware of the significant security breach and potential consequences of allowing an individual not employed by the college to access the college's network for any purpose.

Allowing another individual to access your computer while it is still signed on to your account provides unauthorized network access to the individual and is expressly prohibited. Depending on access rights and privileges extended to the person whose sign-in is used, the unauthorized individual could access employee and/or student social security numbers and other private information, confidential college data and emails, and proprietary information. Further, such access would allow for the theft and/or destruction of such information.

Much time, effort, and money is expended to provide a secure and stable network that protects personal and college data from unauthorized access. We must always be alert to avoiding actions that could compromise our security from within.

The Solution:

Below are three options available to support the need to provide computer access to an individual not employed by the college. An example of when this type of access might be required would be to collect a writing sample from a search and screen candidate.

- Any student PC can be used for this purpose, using the standard student login. Student PCs do not have security access to college information;
- Any college laptop can be used for this purpose. The software is installed locally and does not require a network login.
- If using a networked administrative PC is the only option available, IT can assist by providing a "Guest Account" on the designated machine. A service call must be placed with the helpdesk at least 2 days before access is required. You can contact the helpdesk by phone at x6665 or by e-mail helpdesk@sunywcc.edu. The helpdesk requires the T# of the PC to be used, plus the start and stop day/time that defines the period for which you require the Guest Account.

A Guest Account does not provide access to the network. If printing will be required ensure you have selected a PC that has a printer directly connected, not a network laser printer. As always, insure that there are no personal files stored on the hard disk of the PC, which would be accessible by anyone using the machine. Always use your home drive (H:) for your files and data. A Guest Account cannot access your H: drive.

While we're on the subject of security, please be reminded that your login user ID and password is your key to the electronic door that opens access to all that is yours and the colleges on the network. Please do not share this private information with others, and do not "hang the key on the wall next to the door" by taping or displaying it on your monitor, keyboard, or anywhere else. Our security is only as good as we are at protecting it.

Identity theft, hacked computers, and stolen data are a reality of today's high tech world. Maintaining safe computing practices is our best protection.

Appendix C: (Requesting e-mail and remote access) - Instructions for Requesting Email and Remote Access Accounts for Faculty

When a new faculty member, full-time or adjunct, has completed the hiring process the reporting division or department secretary should fill out the Network Services Request form requesting that the appropriate accounts be created. This is done by using the form located on college's internal website known as Starweb. This link http://starweb.sunywcc.edu/forms/Network_Services_Request.htm brings you directly to the form. The form can only be accessed from on campus or from one of the college's extension sites. The form now requires that the employee ID be provided. For new faculty, the ID can be acquired from the approved hiring PAF. For existing adjunct faculty, the ID can be found on the report of all active adjunct faculty provided by HR and available to all division secretaries on the 'O' drive. In addition, the timekeepers can retrieve the employee ID for existing faculty from the PeopleSoft timesheet. Once the form is completed, clicking on the submit button will send the form to the Information Technology department for processing.

When a request for a new account is received by the Information Technology department the information on the form is reviewed and the appropriate accounts are created. The secretary who submitted the request will be notified as soon as the account has been created and they will be given the User ID and temporary password. This process usually takes less than 48 hours.

The faculty member will pick up their account information from the division or department secretary. The faculty member can then log onto the network and accesses those services that were requested, including email, from on campus. When the faculty member logs onto the network for the first time they will be required to change their network password. Their e-mail password will be synchronized to the new password they have selected. In addition, access to the Library databases are also synchronized with the new password.

To access e-mail from off campus the faculty member must send an e-mail to Ed Kelly and Sean Cole requesting off-campus access for e-mail only **from their college e-mail account** (This insures that a password has been selected). The words "Off-campus access for e-mail" should be in the subject line of the e-mail. The e-mail must include their user ID and office and home phone numbers. For adjunct faculty who do not have an office on campus, only their home phone number is required. When the e-mail has been received with the proper information, access will be provided, usually within 48 hours.

Off campus access to network storage requires the installation of (VPN) security software on the faculty member's home PC or laptop. To request VPN access the faculty member must send an e-mail with "VPN Access" in the subject line to Edward Kelly and Sean Cole **from their college e-mail account**. It must include their user ID and office and home phone numbers. For adjunct faculty who do not have an office on campus, only their home phone number is required. The security software will be provided along with instructions for installing it on their home PC or laptop and for accessing their network storage. The software must be picked up in person as it includes the password required for connecting to the college network and accessing those services requested.

If a faculty member is having difficulty logging in or using email for the first time on campus they should contact Paul Wray at 606-7888 for assistance. Difficulties with VPN access should be reported to the Helpdesk at 606-6665.

Appendix D: (Wireless Access)

Important Note About Access Points:

As a convenience to students and visitors, Westchester Community College provides Internet access through wireless access points, known as the Asgard wireless network, throughout campus and wired jacks at designated locations in the Library.

Use of Asgard is governed by the [Computer Usage Policy](#) of the college, which all students are required to read and agree to upon enrollment.

These wireless connections are isolated from the Westchester Community College data network, and they do not provide protection from others who use the same campus wireless access points or wired jacks in the Library; all such users, in the jargon of networks, are *unauthenticated*; that is, they are connecting to the Internet without logging on to a local area network node and identifying themselves as authorized users of the Westchester Community College-protected local area network.

When you attach to the Internet using these facilities, you must 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 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.

Appendix E: (Certification of Equipment)

Note: If you connect to the internet via Asgard, the college's wireless network, you do not need to have your computer certified. If you attach a computer not owned by the college to a network cable in any classroom, you must have the equipment certified as described below.

Certification of Personal, non-Westchester Community College computing equipment for attachment to Westchester Community College Data Network

- WHO:** All full-time and part-time faculty, guest lecturers, and vendors.
- WHAT:** Certification of non-Westchester Community College computing equipment for connection to Westchester Community College data network
- WHERE:** Westchester Community College
- WHEN:** Once a Semester
- WHY:** Reduce college's risk to attack from computer viruses and worms.

The following procedure applies to computers such as, but not limited to: laptops, tablet PCs, desktop PCs, and notebooks. Under NO circumstances are other types of computing equipment to be attached to the Westchester Community College data network including, but not limited to, routers, hubs, and switches.

You must repeat this procedure at least once a semester if you need continued access to the Internet through the Westchester Community College data network. You must provide a preferred e-mail address for contact if laptops must be recalled for interim certification – for example, if a serious virus or worm becomes public and assurances are required that laptops have received security patches to prevent infection.

Laptops are NOT to be attached to the network unless certified secure by IT, as follows:

- You will bring your laptop to the lab technicians' office in Technology Building, Room 25B. Call 914-606-6995 for information about scheduling the certification procedure.
- You will sign a disclaimer and acknowledgement. The disclaimer removes liability from Information Technology for problems, if any, created in bringing the laptop up to security standards. The acknowledgement acknowledges receipt of the form and understanding of the requirements of the procedure (maintain current security levels, etc.)

The lab technician will:

- Scan laptop for major viruses and clean any found (if possible).

- Install minimum required Microsoft security patches to make the laptop safe for connection to the Westchester Community College wired network.
- Connect laptop to the network.
- Go to Windows Update web site and install any remaining security patches.

If your machine fails at any of these steps, it will not be certified.

The steps outlined above will require a minimum of 20 minutes and possibly as much as 2 hours; if a large number of laptops are submitted for certification, you may be asked to leave the laptop for a period of time, possibly a day or more. Laptops will be processed first-come, first-served. Plan accordingly.

You can greatly decrease the time required to certify your machine if you update your virus definition files, run a full-system scan, and install all critical updates from Windows Update.

In addition, if your laptop has an external CD-Rom drive, include the drive when you present the machine for certification. Also bring the AC adapter so that the machine operates at optimal efficiency during the certification process.

Appendix F: (Saving Files to a Network Location)

FILES SHOULD NOT BE SAVED ON YOUR LOCAL HARD DRIVE (C:)

Saving your files - documents, spreadsheets, databases, presentations & data.

Many have had questions regarding storing files/documents on the local hard drive (C:) versus using the network home directory (H:\My Documents). Hopefully, we can clear up some of the confusion.

Every user has been given personal space on a network server to store files and data. This space is called the home directory and is also called the "H" drive. Listed below are the different areas to store files and data along with their pluses and minuses.

PC's Local Hard Disk - Drive Letters C: and D:

- Files available to all users sitting at PC.
- Unable to retrieve most deleted or corrupted files.
- Files may be deleted or removed during hardware upgrades and replacements.
- Files may be lost in the event of a hardware failure.

Personal Home Directory - Drive Letter H:

- + Backed up nightly.
- + Accessible only to the signed on user.
- + Deleted/Corrupted files can be restored.

Department's Network Directory - Drive Letters I: thru W: (Your department's drive letter may be different).

- + Backed up nightly.
- + Accessible to authorized department users.
- + Deleted/Corrupted files can be restored.

NOTE - Users in Ossining do not have access to campus network storage space. Your documents should be backed up to removable media such as Zip disks or CDs.

The list above shows the importance to saving your files to your "Home" directory or to a department directory stored on the network.

When you save a file in an Office application (Word/Excel/PowerPoint/Access) by using the SAVE or SAVE AS command, the default will be to the H:\my documents folder, please do not change this. Other applications may have to be configured separately. When saving be sure to save to H:\my documents. (Note: Older (DOS) applications may display this folder as H:\my_doc1)

How do I check that my documents are being stored in my home directory?

1. Click Start
2. Click Run
3. Type "H:\My Documents" and click OK.
4. Review the documents stored in your "Home" directory.

If you have any questions about saving files or require additional space, please contact the Helpdesk at x6665.

Appendix G: 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 PCs and the college network. This prohibition also minimizes the risk to college PCs 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.

Appendix I: (Other Items of Interest)

HELP DESK - Have a problem with your PC? Call the Help Desk, x6665. Either your call will be taken by a member of the Help Desk staff, or you will be prompted to leave a message, in which case your call will be returned, typically within 5 minutes. The Helpdesk is staffed from 8:00am - 9:00pm Monday through Thursday and 8:00am - 5:00pm on Fridays. In addition, the IT department has technical and network staff on site until 11:00pm on weekdays and throughout the weekend that will check for Helpdesk voice messages periodically.

E-MAIL - All administrative workstations are connected to WCC's network and have access to Outlook 2007 e-mail. E-mail address format: firstname.lastname@sunywcc.edu

INTERNET - Web access on the Internet is available to all students, staff, faculty, and administrators on network-connected computers and via the College's wireless network. The campus-standard web browser is Microsoft's Internet Explorer. Internet: <http://www.sunywcc.edu> -Intranet: <http://starweb> (only accessible on campus)

MS OFFICE 2007/WINDOWS XP - All campus workstations run under Windows XP, the corporate standard, and have Office 2007 installed.

ACOC - Academic Computing Operations Committee. This committee monitors and manages funds for academic computing software purchases. The Associate Deans and Director of IT have voting authority on all matters. Faculty can request PC software for classroom use through their division office, which is forwarded to ACOC for consideration.

ATC - Academic Technology Committee. This Faculty Senate committee, comprised of faculty representatives from all divisions and IT representation in an advisory capacity, is charged with long range planning for academic computing.

ACADEMIC TECHNOLOGY COORDINATOR - This faculty support position was established in September 1999. This person, Paul Wray, serves as a liaison between our faculty and Information Technology on all academic technology matters, as well as provides technology assistance to our faculty. [Email: paul.wray@sunywcc.edu](mailto:paul.wray@sunywcc.edu). Phone extension: 7888. Office: Adm. B05.

FACULTY FAQ (Frequently Asked Questions) - A document answering the most common faculty questions is available in Outlook Public Folders under Faculty Information.

COMPUTER AND PRINTER REPLACEMENT CYCLE - The standard replacement cycle for desktop computers, laptops, and printers is 5 years.

Appendix J: (Computer Supplies Requests)

For tracking purposes, it is recommended that you make your request for computer related supplies (ink cartridges, toner cartridges, labels, disks, etc) via email to "Supplies". If you do not have access to e-mail you may make your request by calling x6995 and leaving a message. Please include your name and phone number. A request for supplies requires 1 day's advance notice. Requested supplies will be available for pickup in TEC22 after 9am on the day after your request was submitted. You will be notified when your order is ready for pickup. Supplies cannot be sent in interoffice mail.

Supplies Requested on:

Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday

Will be Ready for Pickup on:

Tuesday
Wednesday
Thursday
Friday
Monday
Monday
Monday

Policy on Disclosure of Employee Passwords

At a recent Cabinet meeting, a policy was approved whereby a supervisor needing to obtain an employee's password for access to his/her files must first obtain approval from the appropriate Cabinet member. Even though all material created on College equipment is legally the property of WCC, we do respect the individual's privacy and won't allow access to an employee's files without appropriate need and justification. This policy adds another layer of checks and balances to insure that access isn't provided to another individual inappropriately.

Effective immediately, supervisor requests for password access to employees' files belonging to individuals under his/her supervision require a signature of approval from the Cabinet member of the requestor's division or department on the written request before it will be honored and processed by Information Systems.