INFORMATION TECHNOLOGY EMPLOYEE POLICIES, PROCEDURES & REGULATIONS

THE MISSION AND INTRODUCTION

The mission of the Division of Information Technology at SUNY Westchester Community College is to provide a secure, reliable, and flexible computing environment that facilitates:

- Student learning in and out of the classroom
- Student retention and completion
- The faculty's ability to create and deliver high quality instruction
- The staff's ability to remain agile and operate efficiently supporting faculty and students
- The development of strategies and methodologies that support the mission of the institution

The information systems of SUNY Westchester Community College are made up of heterogeneous systems that are essential to the various workflows that support the day-to-day operations of the College and Strategic initiatives of the institution. All the College systems are comprised of various technologies that allow for students, faculty and staff members to efficiently and effectively perform their required tasks and duties. This document covers the following:

1.1 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, mobile devices, electronic mail ("e-mail"), databases, networks and connection(s) to the Intranet, Internet and any other information technology services available.

1.2 Policies that cover all employees of the College and any other individuals, including consultants, interns, vendors and volunteers, who have access to any College technology assets.

1.3 Inappropriate use of College technology or its services that expose the College to risks including virus/malware attacks, system compromise, interruption of services and litigation is strictly prohibited.

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

SERVICES PROVIDED BY THE DIVISION OF INFORMATION TECHNOLOGY

The following is a list of critical services provided by the Division of Information Technology to College students, administration, staff, and faculty:

- Email
- Internet Connectivity
- Shared File Space
- PeopleSoft (MyWCC i.e., Campus Solutions, Finance, Human Resources)
- Telephone Access (Landline & Mobile)
- Wireless Access
- Printing
- Social Media
- Remote Access via VDI/Horizon Desktop and VPN/Global Connect
- Private and Public Cloud Services
- Degree Works
- Starfish

OWNERSHIP

The College purchases various technology components and services to facilitate the needs of the institution and these items are bound by these conditions:

2.1 All equipment purchased by the College is for the primary purpose of performing official College business.

2.2 All software purchased by the College is for the primary purpose of performing official College business.

2.3 All the data received by the College is for the primary purpose of performing official College business.

2.4 All the data sent by the College to other entities is for the primary purpose of performing official College business.

2.5 Devices not supported or approved by College IT will not be configured for College use.

2.6 Equipment purchased by employees and used for official College business will not be considered a College asset or responsibility.

2.7 Employee procurement of devices and service must be based on the Information Technology approved equipment list (furnished upon request) or receive IT approval prior to purchase, if connectivity to College systems is required.

2.8 Personal devices configured for official College business (e.g., cell phones, laptops, tablets) will only receive partial support for the application/services that has been installed and configured.

2.9 In the event a College or approved personal device is lost or stolen, it must be reported immediately to Campus Security, a police report must be filed, and Information Technology to be disabled/disconnected from the College's information systems and network.

PROHIBITED USE

Improper use of College Systems includes, but is not limited to:

3.1 Contributing to any social media platforms, public forums, chat rooms or message boards except for assigned business or academic related activities (see section below - "Social Media" for details).

3.2 Misrepresenting, obscuring, suppressing, or replacing any identity on an electronic communication.

3.3 Any use or communication in violation of other County, NYS, Federal, and College policies, such as Equal Employment Opportunity policy, Harassment policies, etc.

3.4 Any use of profanity, obscenities, suggestive, intimidating, hostile, discriminatory, or derogatory remarks, even in jest. Using College systems in such a way as to create an intimidating, or hostile work environment.

3.5 Downloading of copyrighted material without specific permission of the copyright owner.

3.6 Downloading or emailing of large files or data for personal use, including video, music, photos, etc.

3.7 The automated forwarding of messages outside of the College. e.g. To your personal email account

3.8 Using College systems to solicit for personal gain, for the advancement of a political or religious belief or for any outside business activity.

3.9 Gambling.

3.10 Any test or attempt to compromise computer or communication system security.

3.11 Any use that violates federal, state, or local law or regulation.

3.12 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.

3.13 Connecting unauthorized equipment to the network or College computers for any purpose or modifying College-issued computer software to function in any other way than specified and/or implemented by the Division of Information Technology.

3.14 Running or installing games or any other unauthorized software, including personal web servers, on College computers.

3.15 The creation of external/internal websites, email distribution groups and social media platforms without expressed permission from the Division of Information Technology.

3.16 Copying of any software from College computers.

3.17 Unauthorized removal or corruption of College data.

3.18 Using the College network to gain unauthorized access to any computer system in and outside of the college.

3.19 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.

PERSONAL USE

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

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

It is the responsibility of each employee and manager to ensure that the college technology is used properly.

LEGAL NAMES TO BE USED WITHIN COLLEGE SYSTEMS

An employee’s legal name as verified by the College’s Human Resources Department will be used in all College information systems. A desired name change should be submitted to Human Resources with the proper documentation to support the change as required by the Human Resources department.

USAGE OF OUTSIDE TECHNOLOGY

As a convenience to students and visitors, the College provides Internet access through wireless access points, known as the ASGARD, ASGARD_Guest and eduroam wireless networks, 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 (i.e. Microsoft Essentials)
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.

INFORMATION SYSTEM USER RESPONSIBILITIES

- Protection of individual account passwords, apart from accounts created for approved College events (not applicable to public access computers).
- Compliance with all laws governing copyright, intellectual property, libel, and privacy (see the College Copyright Policy and Procedures).
- Adherence to the terms of software licenses and other contracts (questions about software license agreements should be directed to the IT Helpdesk).
- Use of College email by employees and trustees as the official means of electronic communication.
- Immediate reporting of loss, damage, theft, or misuse of IT Resources to the College Helpdesk.
- 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 IT.
- Logging off or locking devices or systems when not in use.

COMPUTER & COMMUNICATIONS TECHNOLOGY USE POLICY

A. ***Purpose:***
SUNY Westchester Community College owns and operates a variety of computing systems which are provided for the use of SUNY 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 SUNY Westchester Community College policies.

B. ***Audience & Agreement:***
All users of SUNY 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 SUNY Westchester Community College. SUNY 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 SUNY 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 SUNY 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, except for USB memory sticks, into any computer owned by SUNY 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 SUNY 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 SUNY 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 SUNY Westchester Community College computer system shall be regarded as malicious and may be treated as an illegal act.

Many of the SUNY Westchester Community College computing systems provide access to outside networks, both public and private, which offer 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 SUNY 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 SUNY 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 SUNY Westchester Community College, which is acting solely as the information carrier.

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

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. If an account is compromised, the Division of Information Technology can disable and or change the password for an account to remove access from unknow individual(s).

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 Helpdesk.

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 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.

M. Social Media:

The use of social media to harass, insult, defame, or bully another person or entity; to violate College policy or engage in any unlawful act, but including and not limited to gambling, identity theft, and other types of fraud will result in disciplinary and legal action.

CONFIDENTIAL DATA HANDLING

All individuals associated with the College, in any capacity, are required to handle all College related data in accordance with the following guidelines in mind:

- **Family Educational Rights and Privacy Act of 1974 – (FERPA)**
  - https://studentprivacy.ed.gov/?sr=fpro

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
  - https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

- **Payment Card Industry Data Security Data Security Standard (PCI-DSS)**
  - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1557753660530

- **National Institute of Standards and Technology**
  - https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=904990

- **General Data Protection Regulation (GDPR) – Applies to all European Union Residents ONLY**
  - https://gdpr.eu/data-privacy/

FERPA

In order to ensure that all **Personally Identifiable Information (PII)** is safely handled as per FERPA, the College has classified student data into two categories:

1. Directory Information - Shareable with anyone without the student's consent. *EXCEPTION - a student can choose to "opt out" of having any general Directory Information disclosed to any party.
2. Non-Directory Information – **Not sharable without the student's consent.**

Directory Information	Non-Directory Information
Full Name	Social Security Number
Address	Data of Birth (D.O.B)
WCC Email Address	Personal Email Address
Date of Attendance at the Institution	Place of Birth
Degree Information (including major degrees and academic awards)	Photos, Fingerprints
Enrollment Status (Full-Time / Part Time)	Student ID Number

Please refer to this College site for additional information:
https://www.sunywcc.edu/admissions/registering-for-classes/ferpa/

As a result of the various types of information being stored within various College systems, individuals associated with the College in any capacity should follow these **guidelines when handling NON-DIRECTORY data** with internal and external coworkers/partners:

1. Limit and only share data with individuals or entities within WCC when the data is required to perform their job functions. Include something stating do not share outside of WCC.
2. Only share data in a secure or encrypted fashion.
3. Only save data in secure network folders on the College's network **that are ONLY accessible by applicable personnel who need to work the data**.
4. Do not transmit, collect/store any data within systems that are not owned by the College.

HIPAA

To ensure that all medical related information is safely handled in accordance with HIPAA, the College will only provide medical information to the individual owner of his or her medical records. The only time information can be shared is when the following occurs:

1. The individual presents a serious and imminent threat of harm to self or others, requiring that their medical information be shared with applicable entities (e.g., law enforcement, medical personnel, College personnel) in order to safely prevent any further threats of harm or danger.
2. The individual has given consent to others to receive updates regarding their medical records.

Please note that all medical records are stored within College owned systems are managed in accordance with all HIPAA guidelines.

PCI-DSS

To ensure that all credit card information is safely handled in accordance with PCI-DSS within all College owned and operated systems, all individuals must ensure they use the following tactics when handling such information.

Proper handling of Credit Card Information	Improper handling of Credit Card Information
Only provide credit card information to authorized College systems or offices (e.g. MyWCC, Bursar, Cafeteria, Book Store)	Never write down credit card information on paper
	Never store credit card information within electronic documents (e.g., Word, Excel, Power Point)
	Never provide or accept credit card information via email.
	Never provide or accept credit card information via the phone.
	Never provide credit card information to Non-College owned systems when paying for College services (e.g., google, amazon, ebay)

GDPR – Applicable to European Union (EU) Residents ONLY

All data associated with EU residents is handled in accordance with the General Data Protection Regulations (GDPR) law. The EU consists of the following countries (Qty 28):

European Union Countries	
Austria	Italy
Belgium	Latvia
Bulgaria	Lithuania
Croatia	Luxembourg
Cyprus	Malta
Czechia	Netherlands
Denmark	Poland
Estonia	Portugal
Finland	Romania
France	Slovakia
Germany	Slovenia
Greece	Spain
Hungary	Sweden
Ireland	United Kingdom

https://europa.eu/european-union/about-eu/countries_en

GDPR was adopted by the European Commission in order to strengthen and unify data protection for all EU residents. As per SUNY guidelines, there are two types of information covered under GDPR:

1. Personally identifiable information which mirrors what is covered under FERPA.
2. Sensitive Information – race, ethnicity, political opinions, religious, philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sexual orientation.

As a result of the various types of information being stored within several College systems, individuals associated with the College in any capacity should follow these **guidelines when handling NON-DIRECTORY data** with internal and external coworkers/partners. GDPR does mandate that all College's need a legitimate business purpose to collect and process data.

Please refer to this College site for additional information: https://www.sunywcc.edu/GDPR

The College is bound by various Federal, State, Local laws, and information technology industry standards to protect all data that is handled, stored and/or collected by the College. By following these guidelines, regulations, and laws, an individual will help protect the College from improper data handling and limit the exposure of sensitive student, faculty, and staff data.

UNAUTHORIZED ACCESS

- Allowing another individual to access your computer while it is still signed into your account provides unauthorized network access to the individual and is expressly prohibited.
- At the discretion of the President or Division VP, a manager may be instructed to use another employee's User ID within the same division for a critical business function.

Depending on access rights and privileges extended to the person account, an 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.

Every person is responsible for keeping their workstation and user accounts secure. The following steps should be followed:

- Lock your workstation whenever you leave it, even if you will only be gone for a few minutes.
- It is extremely 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.

PROCEDURE: Locking your Workstation Manually

Press the Windows key (between CTRL and ALT) + the "L" key.

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

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 are 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 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 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, ensure 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 (U:) for your files and data. A Guest Account cannot access your U: drive.

While 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 confidential 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.

PHYSICAL SECURITY

Access to the college data centers and server labs are restricted only to Information Technology personnel. Vendors are only allowed to access these sites with IT management’s approval. Campus Security, Police, Fire, and any other first responders are allowed access without management approval.

As a result of the possibility that sensitive college information could be downloaded on to mobile/remote college devices, employees entrusted with college assets such as desktops, laptops, tablets, mobile devices, and software, must exercise due diligence at all times to prevent theft, destruction or misuse of these assets. Such assets that can store sensitive data are:

- Remote desktops
- Laptops
- Tablets
- Mobile devices
- USB drives
- External hard drives

If any of these items are used by an employee, it is their responsibility to treat these items with care and to safeguard the equipment and information.

Loss or theft of college equipment should be reported to campus security, Information Technology and a police report must be filed.

MONITORING & PRIVACY OF COMMUNICATIONS

The College maintains the right to access and examine College computer systems, 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 ensure that access is not 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 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.

USER ID & 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 the completion of Network Service Request form. The form can be accessed via:

Each person is responsible for all activity that occurs with their User ID. User IDs 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 password changes 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. For security purposes you are forced to change your password every 90 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.

REMOTE ACCESS TO SYSTEMS

The Division of Information Technology provides remote access to various College resources utilizing either VPN or VDI solutions. These solutions are provided by the College and are 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://portal.office.com 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 on 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.

The Division of Information Technology at SUNY Westchester Community College has deployed a Virtual Desktop Infrastructure (VDI) System that provides Staff and Administrators with access to virtual computers on campus accessing routine College systems and applications. The following equipment is needed to access the VDI environment:

- Desktop or Laptop Computer (College Issued or Non-College Issued)
- Broadband Internet Connection

The VDI system can be accessed via two methods:

- Via a Web Browser (e.g., Google Chrome, FireFox)
  VDI-Browser Document - **Does not require any installation of Software.**
  https://1drv.ms/v/s!Ak_Ibkl5wQoQckin2M49S417uPc?e=LAKfDR
  Video Instructions for Web Browser Access

- Vmware Thick Client **(Recommended)**
  VDI-Client Document - **You must have the ability/permission to install software on the computer**
  https://1drv.ms/v/s!Ak_Ibkl5wQoQc9fbTF8Bs0_nxAk?e=Ek8NyH
  Video Instructions for Thin Client Access

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 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://researchguides.sunywcc.edu/c.php?g=707014.

PC SOFTWARE & AUDITING

The installation of software is the responsibility of the Division of Information Technology. The College has the right to audit College personal computers/laptops and remove any unauthorized software.

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.

Users are not permitted to install software on their own unless authorized by the Information Technology Department.

PC AUDITING

Policy:
The Division of 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 the inventory control system.
- For Trial ware: 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 is the user's responsibility. For all College owned networked PCs, IT assumes responsibility for removing trial ware.
- 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 submitted using the personal Software Support Waiver form on http://wcchelpdesk.sunywcc.edu. 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:

- 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.
- 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.

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 (U:\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 "U" 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 U:

+ 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.

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

PROCEDURE:

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 U:\my documents folder, please do not change this. Other applications may have to be configured separately. When saving, be sure to save to U:\my documents.

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

1. Click Start
2. Click Run
3. Type "U:\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 or at helpdesk@sunywcc.edu.

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.

- USB storage devices used by College personnel for College related business, must be hardware encrypted.
- Do not store sensitive or confidential information on unencrypted USB sticks or other portable storage devices.

TECHNOLOGY INVENTORY

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 perform 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 Help Desk at x6665.

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@sunywcc.edu". 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 TEC 27 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 through interoffice mail.

Supplies Requested on:	**Will be ready for Pickup on:**
Monday	Tuesday
Tuesday	Wednesday
Wednesday	Thursday
Thursday	Friday
Friday	Monday
Saturday	Monday
Sunday	Monday

WIRELESS INTERNET CONNECTIVITY

As a convenience to students, administrators, faculty, staff and guests, Westchester Community College provides Internet access via wireless access points located throughout campus.

All users are expected to use wireless access in a legal and responsible manner, consistent with the business and informational purposes for which it is provided.

While using this wireless access, users should not violate federal, State of New York or local laws, including:

The transmission or receiving of child pornography or harmful material. Access to or display of obscene language and sexually explicit graphics is not permitted.

Fraud – Users are prohibited from misrepresenting themselves as another user; attempting to modify or gain access to files, passwords, or data belonging to others; seeking unauthorized access to any computer system or damaging or altering software components of any network or database.

Downloading copyrighted material. U.S. copyright law (Title 17, U.S. Code) prohibits the unauthorized reproduction or distribution of copyrighted materials, except as permitted by the principles of "fair use". Users may not copy or distribute electronic materials without the explicit permission of the copyright holder. By using the wireless network at SUNY Westchester Community College facilities, the user acknowledges that he/she is subject to, and agrees to abide by all laws, and all rules and regulations of the State of New York, and the federal government.

WIRELESS ACCESS

As a convenience to students, faculty, administrators, staff, and guests, Westchester Community College provides Internet access through ASGARD, ASGARD_Guest and eduroam wireless networks, throughout the College.

Use of the ASGARD network(s) is governed by the Computer Usage Policy of the college, which all students are required to read, agree, and adhere to upon enrollment.

Students, faculty, and staff are required to login to the ASGARD wireless network using their College User ID and password.

College visitors are required to go through the registration process and accept the College's "Guest Wireless Access Acceptable Use Policy" before gaining access to the ASGARD_Guest wireless networks.

The eduroam wireless network is a worldwide service initiative that allows students, researchers, and staff members from participating institutions to seamlessly connect to any eduroam wireless network when visiting other participating campuses. This service will also allow visitors to WCC locations to seamlessly connect to the eduroam network with their login credentials from their participating institution.

PROCEDURE:

- Instructions on Accessing ASGARD Wireless Network
- Instructions on Accessing ASGARD Guest Wireless Network
- Instructions on Accessing eduroam International Roaming Network
- Instructions on How to Forget a Wireless Network

Please be advised that when you are connecting to any Wireless Network, you are responsible for protecting your devices against others by practicing safe computing.

This means that at a minimum, you should have:

1. **An up-to-date virus/malware protection software installed.**
2. **All Operating System Security patches installed.**

For more information about safe computing practices, see Protecting Your System.

ALL ELECTRONIC COMMUNICATIONS

All electronic communications provided by the College are property of the College and improper use that violates local/state/federal laws and regulations will result in disciplinary action, as determined by Human Resources. Employees must use extreme caution when opening all forms of e-mail attachments received from unknown senders, which may contain viruses, malware, etc.

Email Content:

- College emails should not contain any private or personal identifiable information (SSNs, birthdates, credit card numbers, course grades, home addresses, phone lists, etc.).
- Emails with personal identifiable information should be deleted from all replies, the original email should be deleted, and future correspondences should not contain such information.
- All correspondence between professors/instructors and students regarding grades and coursework must be done through their official College email accounts. Discussion about grades with individuals other than the student is governed by FERPA.

User Responsibilities:

The Westchester Community College email system is the official channel of communication for College issues. Faculty and staff are responsible for reading their Westchester Community College email account regularly for official college communications. All users are responsible for safeguarding their password and not sharing it with others, including family, friends, supervisors, or colleagues.

Do not use the college's email system for anything other than official college business.

The following e-mail usage and communication activities are deemed as improper and present security risks. The usage guidelines are as follows:

- Do not send 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).
- Do not send any form of harassment via email whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information is prohibited.
- Do not solicit e-mail for any other e-mail address with the intent to harass or to collect replies.
- Do not create or forward "chain letters", "Ponzi schemes" or other "pyramid" schemes of any type.
- Do not post the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Do not email from departmental or shared email accounts when responding to college correspondences. All initiated communications and responses should be sent out from a staff and faculty's email account on behalf of the departmental or shared email account.
- Do not send advocacy emails of any sort using your college email account.
- Do not send emails reflecting political or personal beliefs.

- E-mails/listservs to large groups must include an option and precise instructions, for the recipient to stop receiving the e-mails, also known as opting out.

In order to connect your mobile device to your SUNY Westchester Community College e-mail, you must agree to Information Technology policies related to the use of and storage of WCC e-mails. Some e-mail may contain sensitive or confidential information, and great care should be used when this mail is on a device that is not under the control of the college.

You also agree that SUNY Westchester Community College is not responsible or liable for any problems related to your personal phone.

Social Media Platforms and Instant Messaging Services:

Limited and occasional use of social media is acceptable if it does not violate local/state/federal laws and regulations. The following standards must be adhered to:

- Used in a professional and responsible manner.
- Is not detrimental to the college's best interests.
- Does not interfere with an employee's regular work duties.
- Not to be used to engage in any social media communications that may harm or tarnish the image, reputation and/or goodwill of the college and/or any of its employees.
- Not to be used to make any discriminatory, disparaging, defamatory or harassing comments that is prohibited by the college's Non-Discrimination and Anti-Harassment policy.
- When Employees express their beliefs and/or opinions on social media, the employee may not, indirectly or implicitly, represent themselves as an employee or representative of the college.
- Employees assume all risk associated with social media.
- Do not use the College's trademarks, logos, or College-owned intellectual property with any social media outlet.

Any violation will result in disciplinary action as determined by Human Resources.

RAVE ALERT SYSTEM

The College Rave Alert system is an alert system that is used by College Relations, Student Involvement, and Security to inform the student, faculty, administrators, and staff via text message, phone call, and email about college related incidents that affect the workflow (i.e., inclement weather closings/advisory, major incidents, major student events and/or safety of those who travel to the main campus and extension sites).

RAVE RECOMMENDATIONS

Westchester
Community College
State University of New York

Dec 8, 2014
The Cabinet made the following recommendations:

- Texts, emails, and phone messages would be sent to faculty and staff about weather-related closings. Additional clarifying information will be sent to the campus about how to make desired changes to personal contact information in PeopleSoft.

- Students would receive text messages and emails about weather related closings.

- In an emergency, all methods of communication would be used with faculty, staff, and students that will include texts, emails, and phone messages.

DIGITAL SIGNAGE SYSTEM

All digital displays in common areas of the College and Extension hub locations are required to be connected to the College's Digital Signage System. This will allow security to take control of all signs during an emergency and provide a uniform look across the entire College.

DIGITAL SIGNAGE SYSTEM POLICY

Westchester Community College
State University of New York

Policy: Digital Signage System

Date: 11/3/2014

On Monday, October 27, 2014 the Cabinet approved all digital displays in common areas of the College and Extension hub locations are required to be connected to the College's Digital Signage System. This will allow security to take control of all signs during an emergency, and provide a uniform look across the entire College.

All new digital signs must be purchased with the appropriate hardware to connect to the Digital Signage system. All existing signs not connected to the Digital Signage system, must be connected to the Digital Signage system by August 31, 2015.

MOBILE DEVICE & EMAIL

Westchester Community College
State University of New York

The Division of Information Technology

Mobile Device/OWA (Outlook Web Access) E-mail: Declaration

By connecting your mobile device to your Westchester Community College e-mail, you agree to all Information Technology polices related to the use of and storage of WCC e-mails. Some e-mail may contain sensitive or confidential information, and great care should be used when this mail is on a device that is not under the control of the College.

You also agree that Westchester Community College is not to responsible or liable for any problems related to your personal phone.

The College’s e-mail system has a “device wipe” feature. This feature allows the e-mail administrator to send a command to a handheld device to remove mail. This command may also reset the phone or device to its default configuration. Thus, not only is WCC e-mail removed, but all personal information could possibly be removed, including accounts set up on your phone, other e-mail accounts, contacts, and even Apps that you may have added. The process can also remove all history and clear your memory card. This feature would be used if the phone is reported lost or stolen or when you are no longer employed at the College. For this reason, you agree that Westchester Community College is not responsible for or required to replace or service any such device in the event of any information or configuration loss.

The following steps are required if you agree to connect your device to Westchester Community College e-mail servers.

- Your handheld, phone or other device must be password protected. This password protection should be set up to protect your device with a timer in case you put your phone down, or the device is lost or stolen.
- Back up your device often. Some applications, Gmail for example, will store names and contacts for you. Some application searches, “Apps Brain”, for example, will keep a history of your Apps and allow you to reinstall them. Pictures and downloads should also be regularly backed up from your phone.
- You should note any other configuration changes or add-ons you have installed on your device.
- When you leave the College’s employ, you will remove your connection to WCC mail.

The Division of Information Technology at Westchester Community College does not take responsibility for or provide support for devices not purchased by the college.

________________________________ ________________________________

Print Name Date

____

Signature

USAGE OF INTERNET CLOUD STORAGE

The usage of any cloud-based storage is prohibited when handling data that is specific to the college and student information. Any such usage would violate the Family Education Rights and Privacy Act (FERPA).

Westchester
Community College
State University of New York

The Division of Information Technology

Using Internet (Cloud) Storage: Declaration

As an employee of Westchester Community College, I agree to abide by the regulations established by Information Technology by **not** using Internet features such as Dropbox and OneDrive (or similar service) to store any confidential student or personnel data. I understand that any violation of this agreement constitutes a violation of the Family Educational Rights and Privacy Act (FERPA), a federal law.

(For more information about FERPA requirements, see the College's website: www.sunywcc.edu).