Table of Contents

IT Code of Conduct 2
- Cell Phone Policy 2
- Classroom Audio/Video Recording Policy 2
- Information Technology Hardware Requirements 2
- Information Technology Software Requirements 2
- Student Computer and Account Use Policy 2
- Cyber Security Awareness Resources for Students 3
- Copyright Infringement 4

Verification of Student Identity (Distance Education) 5

IT CODE OF CONDUCT

Cell Phone Policy
Making calls in classrooms is not allowed. If an emergency call must be made, the student should request permission from the instructor to leave the classroom in order to use the cell phone. Discrete use of cell phones is allowed in public areas only.

Classroom Audio/Video Recording Policy
In order to respect and ensure the privacy of faculty, staff, and students, The College of Westchester prohibits students from recording others in the classroom via audio or video without the consent of all parties being recorded (see general policy prohibiting recording under the section titled *Grounds for Disciplinary Action).* Notwithstanding the foregoing, faculty reserve the right to grant permission for students to photograph content written or displayed on classroom whiteboards. Students needing academic accommodations in the classroom may be granted permission through the Coordinator for Accessibility Services to record classes and lectures. When prior approval to record whiteboards, lectures, or course discussions is granted, the recorded materials are for personal academic use only and are not for public distribution or sale in any fashion.

Information Technology Hardware Requirements
It is mandatory for students to possess a computer device with internet capabilities to access vital application systems, such as D2L Brightspace, our Learning Management System (LMS) and Microsoft Office 365, which all students are entitled to download at their convenience. Both the LMS and Office 365 are compatible with computers, tablets, and smartphones, though some application features may be less practical on a smartphone. Devices must maintain a reliable internet connection, operate effectively without any malware, and have an updated operating system to properly engage with these essential services.

Students should be aware that certain campus-based Academic Programs may require additional hardware and software, which are provided within our on-campus computer laboratories.

Students enrolled in Online and Evening Programs are expected to consistently have access to a capable device that supports internet browser-based applications. The same is highly recommended for students in Day Term Programs. For those in need, there is a finite quantity of computers accessible on Campus.

Information Technology Software Requirements
For the Learning Management System Platform (D2L Brightspace):
We recommend utilizing the most current versions of Microsoft Edge, Chrome, Firefox, Internet Explorer, or Safari to optimize your experience on the platform. Although the platform might operate on other browsers, optimal performance is assured with the ones previously mentioned.

For MS Office Products
The College of Westchester incorporates Microsoft Word, Excel, and PowerPoint across various courses. The following link offered by Microsoft details the system requirements for these applications: Office System Requirements. Students from The College of Westchester have the privilege to obtain and install MS Office 365 by navigating to https://portal.office.com and entering their college-provided email and password. Eligible students can install MS Office 365 on up to five different devices and maintain access throughout their active enrollment at the institution.

Student Computer and Account Use Policy
This policy applies to all students who have been assigned a user account or access, use, or store information on any of The College of Westchester (College) computer resources, whether on campus or remotely, for academic or personal purposes. Students are expected to comply with this policy, as well as with all applicable laws, regulations, and College policies and procedures. The policy also applies to any devices, networks, and systems that students use to access the platform and resources, whether owned by the College or by the students themselves.

Students are responsible for:
- Using their accounts only for authorized and legitimate educational purposes.
- Keeping their usernames and passwords confidential and secure, and not sharing them with anyone else.
- Logging out of their accounts and closing their browsers when they finish using the platform and resources.
- Following the College's policies and rules regarding academic honesty, plagiarism, copyright, privacy, and communication.
- Respecting the rights, opinions, and dignity of other students, teachers, and staff on the platforms and resources and conduct themselves in a manner that does not violate any applicable laws, regulations, or ethical standards.
- Using the platforms and resources in a manner that does not harm, disrupt, or interfere with the normal operation and performance of the platforms and resources, or the devices, networks, and systems of the College or other users.
- Reporting any suspected or actual unauthorized access, misuse, or breach of their accounts, or violations of this policy, or any incidents or problems related to any College computer resource to the College immediately.

Students are prohibited from:
- Using a College account, resource or communication to access, create, store, transmit, or distribute any content that is illegal, harmful, offensive, abusive, harassing, threatening, defamatory, obscene, vulgar, hateful, discriminatory, or otherwise inappropriate.
- Using a College account, resource or communication to impersonate, deceive, or misrepresent themselves or others.

- Using a College account, resource or communication to solicit, advertise, promote, profit from, or endorse any products, services, or organizations that are not related to the College or the educational purposes of the platform and resources.
- Using a College account, resource or communication to engage in any activities that are disruptive, malicious, fraudulent, or criminal, such as hacking, phishing, spamming, spoofing, or distributing viruses, malware, or other harmful software or code.
- Using a College account, or resource to access, modify, delete, or damage any data, files, or systems that belong to the College or other users, without proper authorization or consent.
- Using a College account, resource or communication to bypass, circumvent, or disable any security measures, controls, or restrictions that are in place on the platform and resources, or the devices, networks, and systems of the College or other users.
- Using a College account, or resource to download, install, or run any software, applications, or programs not authorized by the College.
- Using a College account, or resource to violate the intellectual property rights of the College or other users, such as copying, reproducing, distributing, or modifying any content, materials, or information without permission or attribution.

Mandatory Multi-Factor Authentication (MFA):
All CW accounts are protected by mandatory Multi-Factor Authentication (MFA). Enrollment in MFA is required for all users and cannot be opted out. Access to College systems, platforms, and resources will only be granted after successful MFA verification. Students must follow all instructions for MFA setup and maintenance; and promptly report any issues with authentication to the College helpdesk.

The College of Westchester provides students with a range of electronic communication tools and applications that support their academic pursuits. These facilities encompass, among others, computing hardware, telephonic devices, electronic mail (email), internet connectivity, along with various communication applications and technologies (such as text messaging, instant messaging, etc.) utilized by the College. The use of these resources is exclusively reserved for educational purposes and they and their data remain under the ownership of the College.

By accessing the internet, network, Microsoft 365, online learning platform Internet, or any other digital resources at the College, whether using a College account or not, students acknowledge that they have read, understood, and agreed to this policy and the terms and conditions stated herein. Students also acknowledge that they are solely responsible for their actions and the consequences of their actions on the platform and resources, and that they will comply with this policy and any other policies or rules of the College, and any applicable laws or regulations, at all times.
The College reserves the right to access and review all content on its systems and does not guarantee privacy for password-protected messages. It retains the authority to monitor and manage usage of its electronic communication systems as they relate to the College. The College reserves the authority to release any data or information transmitted through its networks, with or without prior notification.
The College reserves the right to monitor, audit, and review any activities, data, files, or communications that are conducted or stored on the platform and resources, or the devices, networks, and systems of the College or other users, using the student accounts, in accordance with the College's policies and applicable laws and regulations. The College also reserves the right to reassign, reuse, publish, or share a student's account principle name (ex: unique_identifier@students.cw.edu), with or without the sub-domain name, at the College's discretion. The student's account is the sole property of the College. The College is not liable for any loss, damage, or liability that may result from any violations of this policy, or any unauthorized or improper use of the resources by the students or any third parties.

It is your responsibility to comply with this policy. Failure to do so may result in disciplinary action as listed in this policy's Non-Compliance section.

Non-Compliance:
Violations of this policy will be treated like other allegations of misconduct at The College of Westchester. Allegations of misconduct will be adjudicated according to the *Disciplinary Grievance Procedures for Conduct Violations*. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable The College of Westchester policies.
2. Termination, suspension, and/or revocation of any student accounts.
3. Report any violations to the relevant authorities and cooperate with any investigations or legal actions that may arise from such violations.
4. Legal action according to applicable laws and contractual agreements.

College Use of Email
Email serves as an official channel of communication at The College. As such, the institution reserves the authority to disseminate information to students via email and anticipates these messages will be promptly received and reviewed. Instructors have the discretion to decide how email will be utilized in their courses. It is expected that students regularly monitor their official email account to remain informed about college-related matters. The College advises reviewing emails at least twice weekly, acknowledging that some announcements may be urgent.

Cyber Security Awareness Resources for Students
A range of Cyber Security Awareness videos for students is accessible via the CW Everywhere app. With a dedication to enhancing cyber security knowledge, The College plans to add more materials on the student platforms. Students should watch for updates about these resources in their college emails and other school communication channels.

Student Support
For 24/7 phone assistance with system access issues, students should dial (877) 461-0043. To receive assistance during the College's operating hours, contact helpdesk@cw.edu via email.

Copyright Infringement
"As a general matter, copyright infringement occurs when a copyrighted work is reproduced, distributed, performed, publicly displayed, or made into a derivative work without the permission of the copyright owner." (http://www.copyright.gov/help/faq/faq-definitions.html)
Copyright infringement includes downloading and reproducing CDs or DVDs for commercial distribution, removing notice of copyright or distribution of any article with copyright notice removed. There are federal laws that protect copyrighted materials from unauthorized use or distribution. Federal penalties associated with copyright infringements may be either civil or criminal. Under a civil lawsuit the copyright owner may file (1) to recover actual damages and additional profits, costs and attorney fees or (2) statutory damages for all infringements, which can be as high as $150,000. Under the "No Electronic Theft (NET) Act," criminal penalties for unauthorized software duplication can result in being fined up to $250,000 or up to five years in prison even when there is no monetary gain. Individuals who are found to be guilty of "peer-to-peer file sharing" may be subject to prosecution as a criminal. Sharing copyrighted materials without a license (e.g., P2P file sharing which is often automatically shared) is against the law and also prohibited under this policy and subject to discipline. Copyright abuse can subject both the user and The College to legal sanctions. Federal law requires The College to take action when it is notified that someone on its network is distributing copyrighted materials. The College will not protect any individual users, faculty, staff or students who distribute copyrighted material without license. Additionally, repeat infringements of copyright by a user can result in termination of the user's access to College systems and networks.

Authorized representatives of The College may monitor the use of the electronic communication systems to ensure that use is consistent with educational needs; they may also override all passwords or security codes when deemed necessary.

- The College may from time to time, as it deems necessary in the ordinary course of business, monitor students' use of the electronic communication systems.
- No users of The College's electronic communications systems shall use such systems to violate or infringe upon the copyright of any third party.
- The equipment, services, and technology provided to access the Internet or other electronic communication devices remain at all times the property of The College. The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited.

All electronic communications are part of The College's records and, as such, may be disclosed without The College's permission. Therefore, students should not assume that any communication is "private," even if the student designates the message as such.

Students are responsible for safeguarding their log-on and other passwords or security codes. They may not share these codes with any third party or with another student. The College of Westchester makes no warranties of any kind, whether expressed or implied, for the information systems and communications services it is providing, and will not be responsible for any damages users suffer including loss of data.

All parties who use The College's electronic communication systems are deemed to have accepted this policy and are required to comply with it. Any student who violates this policy or uses the computer, other electronic, or telephone systems for improper purposes shall be subject to discipline, up to and including termination. Students are responsible for reporting any violations of this policy to the Director of Administration. This policy is published in compliance with the Higher Education Opportunity Act, which requires institutions to disclose information regarding copyright infringement and the unauthorized distribution of copyrighted materials, including peer-to-peer file sharing.

Verification of Student Identity (Distance Education)

The College of Westchester verifies student identity in online and distance education courses through secure authentication processes to ensure that the student who registers for a course is the same student who participates academically.

Student identity is verified through the use of unique College-issued credentials and mandatory Multi-Factor Authentication (MFA) for access to the College's learning management system and institutional platforms. MFA enrollment is required for all students and cannot be waived. Detailed requirements governing MFA, system access, monitoring, and acceptable use are outlined in the College's IT Code of Conduct, (Student Handbook Addendum pg. 2) which is incorporated herein by reference.

The College does not charge students any additional fees for identity verification related to online or distance education courses and does not require students enrolled in distance education courses to travel to campus for identity verification. Any future changes to identity verification practices or associated charges will be disclosed to students in writing at the time of registration or enrollment.