ADMINISTRATIVE POLICY
STUDENT AFFAIRS
STUDENT ACCEPTABLE USE OF TECHNOLOGY
STU-401

OWNER(S): Executive Director, Information Technology Services/(CIO), Dean of Students
UPDATED: February 2026

PURPOSE

The College provides students with access to certain of the College's approved computers, printers, e-mail systems, telephone systems, video conferencing systems, other hosted systems, student accounts, software, online storage media, College data and data networks, and artificial intelligence (AI) tools, internet access, wired and wireless networks, and institutional and departmental information systems, which we call "technology resources."

The purpose of this Student Technology Acceptable Use Policy ("AUP") is to (a) protect the technology resources, (b) satisfy the College's legal obligations, (c) support academic integrity, and (d) help ensure that the use of the College's technology resources is consistent with the College's mission and values.

When in doubt, always contact the ITS Department first to confirm if your use of our technology resources is acceptable.

SCOPE

This AUP applies to all students who have College-supplied account credentials (student ID and password) that permit them to use the College's technology resources.

PROHIBITED USES OF COLLEGE TECHNOLOGY RESOURCES

Technology resources may be used only in a manner consistent with the College's mission, policies, and legal requirements and only for their authorized purposes, which are to support the educational, clinical, administrative, and other functions of the College.

Students are prohibited from using the College technology resources in any of the following ways:

- **Violations of Law:** Using College technology resources in a manner that violates applicable laws, including but not limited to laws related to harassment, stalking, threats, copyright infringement, unauthorized access to computer systems, or distribution of illegal materials.
- **Academic Dishonesty:** Using College technology resources to plagiarize, cheat on exams or assignments, submit work that is not your own, share answers or course materials inappropriately, or otherwise violate the College's academic integrity policies. This includes using AI tools to complete assignments when your instructor has prohibited their use.
- **Infringement of Intellectual Property:** Using College technology resources to create, share, or distribute materials that violate the copyright, patent, or other intellectual property rights of another person or entity without the owner's permission or in violation of the College's Intellectual Property Policy.
- **Unauthorized Sharing of Accounts or Credentials:** Sharing College-issued account(s), student ID(s), or password(s) with anyone else, or allowing others to access any such information. Students are responsible for all activities that occur under their account credentials. Sharing account credentials to complete coursework is considered plagiarism.
- **Unauthorized System Access, Testing, or Impersonation:** Accessing or attempting to access College technology systems, applications, databases, or network resources beyond the scope of

student's authorized role; impersonating any other user (student, faculty, staff, or administrator); using technical knowledge or tools to circumvent access restrictions or authentication mechanisms; or engaging in any activity that exceeds student's authorized level of access. A student's technical ability to access a system does not constitute authorization to do so.

- **Attempts to Defeat System Security**: Students must not defeat or attempt to defeat any technology resource security. Examples are "cracking" or guessing and applying the identification or password of another user; compromising room locks or alarm systems; breaching or testing computer or other electronic media security measures; defeating or testing anti-virus, anti-spam, or other filters; or interfering with the operating system or software application patching process. This provision does not prohibit ITS from using security scan programs within the scope of their responsibility.
- **Generating or Distributing Harmful or Malicious Content:** Using any technology resources to create, support, or distribute viruses, malware, worms, or other rogue programs; or engaging or attempting to engage in phishing attacks, data scraping, spam, cyber scams, or cyberattacks.
- **Generating Bias, Discrimination, or Harassment:** Using technology resources to create, share, or distribute content that is hateful, abusive, biased, discriminatory, harassing, threatening, or offensive, including by reference to sex, race, national origin, gender, religion, age, disability, veteran status, sexual orientation, or any other legally protected category.
- **Misinformation and Deception:** Using College technology resources to generate or distribute content intended to mislead, deceive, or manipulate individuals, including the creation of deepfakes, fake news, or false information.
- **Inappropriate Content:** Using College technology resources to collect, create, use, share, or store video or audio recordings, images, or digital content that are illegal, unethical, fraudulent, profane, obscene, sexually explicit or graphic, defamatory, derogatory, hostile, or otherwise offensive or inappropriate in an educational environment.
- **Overreliance on Technology Resources:** WCTC provides College technology resources, including approved AI tools, to assist students in their learning. However, using these College technology resources is not a substitute for developing student's own knowledge and critical thinking skills. Because AI tools are still in the early stages of development, the output created using AI tools may be wrong or incomplete. For instance, some AI tools are said to "hallucinate," meaning they "make up" information when preparing responses to requests. Students must always verify the accuracy of output from College technology resources, including AI tools.
- **Commercial Use or Advocacy:** Using College resources to solicit money or other items or generate unsolicited marketing without the prior written permission of the College or using College resources for political activity, fundraising, or lobbying efforts.
- **Use of unauthorized Software and Unauthorized Devices:** Downloading, installing, or deploying software code within the College's IT systems without prior written approval of the ITS Department or uninstalling/disabling WCTC installed software without approval of the ITS Department. All College software must be properly licensed and purchased through approved purchasing methods. Physically connecting additional devices, including but not limited to PCs, laptops, routers, network switches, wireless access points, network servers, network sniffers, or external devices for additional data storage or backup of data, printers, or video or voice systems to the College's IT systems without prior written approval of the ITS Department.

- **Interference with College IT Systems:** Using any College technology resources to harm, disrupt, or otherwise interfere with the operation of the College or its IT systems, to circumvent the College's IT systems, to gain unauthorized access to College data, to delete, modify, or destroy College data, or to bypass or subvert the College's security protocols.
- **Use that Impedes, Interferes with, Impairs, or Otherwise Causes Harm to the Activities of Others:** Students must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Other behavior that may cause excessive network traffic or computing load is also prohibited.
- **Leaving Devices Unattended:** Leaving any College-issued computer or other electronic devices unattended without either logging out or locking the device. If a previous user leaves their access open, you must log out of that current session before starting a new session.

INSTRUCTOR GUIDELINES FOR TECHNOLOGY USE

Instructors may establish and communicate clear guidelines for using College technology resources, including AI tools, in their courses. These guidelines will be provided in the course syllabus or other course materials. Students are responsible for understanding and following instructor's specific technology use policies for each course. If an instructor does not allow the use of AI tools or other technology resources and students use them anyway, this may constitute academic dishonesty.

ACADEMIC INTEGRITY AND TECHNOLOGY USE

Use of technology resources must support, not undermine, academic integrity. Students are responsible for ensuring that all work submitted is their own, even when using technology resources to assist them. When students use AI tools or other technology resources to help with assignments, they must:

- Follow their instructor's specific guidelines for that course and assignment
- Cite any AI tools or resources used, as directed by their instructor
- Understand that they are responsible for the accuracy and quality of all work submitted, even if technology helped create it
- Remember that using AI or other technology to complete work an instructor expects students to do themselves is academic dishonesty

USE OF THE COLLEGE'S IT SUPPORT TEAM AND TECHNOLOGY RESOURCES

When students interact with the College's IT Support Team, they are expected to do so in a manner that comports with all College policies and expectations. Students must not waste College technology resources or purposefully damage or deface any College equipment. Students are responsible for the reasonable care of any College equipment checked out to you.

COLLEGE MAY MONITOR TECHNOLOGY RESOURCES

The ability to use the College's technology resources is a privilege, not a right. The College has the right to monitor any communications or actions students take when using technology resources. Any documents,

records, materials, files, content, or communications that students create, send, or store using technology resources are available to the College, and students have no expectation of privacy in those items, except as provided by law.

INCIDENT REPORTING

If you become aware of any actual or suspected violation of this AUP, a security incident, or a data breach, you must immediately report that information to the Dean of Students via the College's official reporting system, to your instructor, or to the ITS Department. You should also report any suspicious emails, unusual system behavior, or potential security threats.

WHO TO CONTACT

If you have questions about:

- Technology resources, access, or technical support: Contact the ITS Help Desk
- Whether you can use a specific tool for an assignment: Ask your instructor
- This policy in general: Contact the ITS Department
- Reporting a policy violation or security incident: Contact the Dean of Students or ITS Department

POLICY COMPLIANCE AND ENFORCEMENT

If you do not comply with this AUP, you may be subject to:

- Loss of access to College technology resources
- Academic consequences, including academic dishonesty proceedings
- Disciplinary action under the Student Code of Conduct, up to and including suspension or expulsion
- Legal action if your conduct violates federal, state, or local laws

The College may temporarily suspend your access to technology resources while investigating potential violations of this policy.

POLICY REVIEW

The Executive Director, Information Technology Services/Chief Information Officer (CIO) and Dean of Students will review this AUP semi-annually during each calendar year and propose updates to keep up with technological changes.