



Committee Meeting: Policy & Governance Committee	Date: January 12, 2026
Committee Chair: Melodie Baker	
New or Edited: Edited	

**POLICY NAME:** Acceptable Use Policy

**POLICY TYPE:** Managerial

**SUBMITTED BY:** Daniel Bartkowiak, Information Security Officer

**ISSUE OR STATEMENT OF PURPOSE:** SUNY Erie Community College (“SUNY Erie” or “the College”) respects individual privacy, civility, intellectual property rights, and academic freedom. The College provides students and employees broad access to information and technology resources in support of instruction, learning, research, communication, and the overall mission of the institution. As technology continues to evolve, SUNY Erie recognizes that responsible access to these resources is essential to the free exchange of ideas and opinions fundamental to higher education.

This Acceptable Use Policy (AUP) defines the expectations and responsibilities of all individuals who use SUNY Erie’s information and technology resources. Every member of the SUNY Erie community shares responsibility for using these resources properly, lawfully, and ethically. Technology resources are provided primarily for educational and institutional purposes and must be used in compliance with applicable federal, state, and local laws and regulations, including but not limited to FERPA, GLBA, PCI DSS, the New York State Information Security Breach and Notification Act, SUNY Policy 6900, and SUNY Erie’s Information Security Policy (ISP).

The AUP has undergone significant revisions in response to the adoption of SUNY Policy 6900 and the development of SUNY Erie’s ISP. Historically, the AUP functioned as the primary ITS policy governing user behavior. As part of a broader maturation of the College’s information security program, certain requirements have been relocated to the ISP, others have been clarified or updated, and new provisions have been incorporated to address emerging technologies, risks, and regulatory expectations. Together, these policies are intended to safeguard privacy, protect College networks, systems, data, and software, ensure proper care of equipment, and promote the responsible stewardship of public resources.

**NEW OR EDITED POLICY:** Edited

**POLICY:**

**Scope:**

Information Technology Services (hereinafter “ITS”) provides and maintains the campus network, servers, computer labs and facilities, and College-owned equipment such as telephones, desktop and laptop computers. ITS provides additional services, including the operation of a Help Desk, tutorial assistance, audio visual services and educational technology resources and support. These facilities and technological resources and



**POLICY NAME:** Acceptable Use Policy **Continued**

services provided through ITS are a crucial resource for academic and administrative members of the college community.

Since no list can cover all possible circumstances, the spirit of this Acceptable Use Policy must be respected—namely, avoiding any action that interferes with legitimate equipment usage, impedes one’s work performance, unnecessarily circumvents security measures, invades the privacy of another person or institution, or uses SUNY Erie resources for non-College business.

**Acceptable Use Policy:**

All employees, contractors, volunteers, and students are responsible for exercising good judgment regarding appropriate and reasonable use of information, electronic devices, and network resources in a manner that complies with SUNY Erie’s policies and procedures, as well as local laws and regulations.

**Use of SUNY Erie’s ITS resources constitutes an agreement to abide by this Acceptable Use Policy.** Users found in violation may be subject to penalties of varying degree, and violators may also be subject to action by the College, as well as civil and/or criminal judicial systems, as appropriate.

**User Responsibilities and Privacy Considerations:**

All college faculty, staff, and students are afforded the privilege of access to the computing and network resources/equipment of the College. Such access may be granted to other individuals and groups, but only with approval from ITS or authorized personnel. All parties are responsible for preserving the integrity of the College’s technology resources and using them in a manner consistent with this policy and any other applicable SUNY Erie policies, as well as relevant federal, state and local laws and regulations.

- Users accept responsibility for learning how to use information technology effectively and responsibly. The College provides training on the use of information technology. All users are encouraged to learn the proper use of information technology through individual learning or by attending training sessions or classes.
- Users accept responsibility for backup and security of their work. Each user should learn how to make backup copies of important work and to properly use software features for securing and/or sharing access to their information.
- Users must avoid the use of external services, such as artificial intelligence platforms, for processing or analyzing non-directory Student Records and other sensitive SUNY Erie data, unless explicitly approved by the College. Special care must be taken to avoid unauthorized disclosures or data exfiltration risks.

**Equipment, Facilities, Account, & Network:**

**Equipment**

Any equipment (e.g. laptops, desktop computers, tablets, cell phones) assigned to students, contractors, faculty and staff for the duration of their employment or agreement at SUNY Erie remain the property of the College and should be treated as such. These devices may be upgraded, as warranted, and must be relinquished in order for any required repairs or updates to be performed.



**POLICY NAME:** Acceptable Use Policy **Continued**

SUNY Erie resources—including email accounts, computers, and other electronic devices—are intended strictly for College-related business. To maintain compliance with institutional policies and safeguard College systems, all personnel are strongly advised to use personal email accounts and devices for any non-work-related activities.

Failure to follow this guidance may result in unintended consequences. In the event of equipment failure, suspension, or termination of employment, access to College-assigned accounts, computers, and devices may be immediately revoked without notice. Users should avoid relying on College resources for personal matters to prevent disruption or loss of access.

Voluntarily separating employees should review the “SUNY Erie’s Off Boarding Policy” to review the process for returning of technological equipment.

**Use of College Technology Facilities**

SUNY Erie’s technology resources—including those located at remote sites—are provided to support the academic, administrative, and operational needs of the College. These facilities are intended for use by SUNY Erie students, employees, Trustees, and other individuals who have been granted authorized access. All users are expected to use these resources responsibly and in alignment with the College’s mission and policies.

- Users must not abuse equipment and are asked to report any mistreatment or vandalism of computing or network facilities to ITS staff or to Security.
- Food is discouraged in all computing facilities because of potential harm to equipment. Beverages are permitted only in sturdy, spill-resistant containers—such as reusable bottles with secure lids or travel mugs. Disposable cups without lids, open containers, or anything prone to leaking are not allowed near technology equipment.
- Shared equipment should not be monopolized. Users must relinquish the computer they are using if they are doing nonessential work when others are waiting for a computer to perform course or work-related activities. Users are prohibited from using more than one computer at a time and should plan work so that their computer session is no longer than necessary.
- Users shall not run unapproved software, alter system files, move, or disconnect any cables on computers or other equipment. ITS tickets will be needed for any of these tasks.
- All users are expected to treat fellow students, staff, and lab personnel with respect and professionalism. Harassment, intimidation, or abuse—whether verbal, physical, or digital—will not be tolerated. This includes cyberbullying, unwanted messages, or any behavior that disrupts the learning or working environment.
- Users are expected to follow all posted notices within technology facilities, including those related to hours of operation, printing procedures, equipment usage, and other operational guidelines. These notices are in place to ensure fair access, maintain equipment integrity, and support a productive environment for all users.

**Account Usage**

- Account holders must not allow others to use their personal SUNY Erie accounts. The person assigned an account is wholly responsible for its use, and all activity originating from that account, at all times.



**POLICY NAME:** Acceptable Use Policy **Continued**

- Sharing passwords or allowing others to access your account is strictly prohibited. Any attempt to gain unauthorized access to another user's account or to determine their password may result in disciplinary action and/or suspension of access.
- Account holders must use SUNY Erie's email, forums, and other communication systems responsibly and professionally. Communications should serve a legitimate academic or administrative purpose.
- Users are required to identify themselves accurately in all electronic communications. Anonymous postings, impersonation, or spoofing of email addresses is not permitted.
- With HR approval employees and contractors who have separated from the College may be provided access to their accounts for a specified period upon approval.

**Network Usage**

The following are responsibilities that are particularly applicable to users of SUNY Erie's campus-wide network.

- Only ITS devices can be plugged into the campus network. Users cannot plug a personal laptop or device into a campus Ethernet port. Unauthorized devices will be blocked automatically.
- Attempts to bypass these controls, such as spoofing a device's identity, using unauthorized network switches, or connecting unapproved equipment, are considered violations of College policy.
- The person recognized as the owner of an authenticated computer system is responsible for that computer's use, and for all activity originating from that computer, at all times.
- Excessive or improper use of network resources that interferes with or degrades access for others is strictly prohibited. This includes activities that consume disproportionate bandwidth, disrupt normal operations, or violate SUNY Erie's acceptable use standards. Examples include running peer-to-peer file sharing applications, using anonymizing services such as Tor or VPNs to bypass network restrictions, or hosting unauthorized services or servers on the College network.
- Any user that brings their non-SUNY Erie owned equipment onto SUNY Erie property must still abide by this policy while using those devices.
- Under no circumstances may users connect unauthorized servers to the SUNY Erie network. This includes, but is not limited to, servers that provide network services such as DNS, DHCP, BOOTP, or any other service that assigns or manages IP addresses or interferes with network traffic. Any attempt to introduce rogue servers, bypass network controls, or disrupt network operations is strictly prohibited.
- Due to the significant risk of network disruption caused by unauthorized or misconfigured networking equipment, the use of personal routers, wireless access points (WAPs), or any device that functions as a router or WAP is strictly prohibited on the SUNY Erie network. Only networking devices deployed, configured, and managed by ITS are permitted.
- Use of AI tools, bots, or agents to conduct vulnerability scanning, penetration testing, port scanning, identity enumeration, or any other form of automated network reconnaissance is strictly prohibited.



**POLICY NAME:** Acceptable Use Policy **Continued**

**Legal Usage**

Information technology resources may not be used for illegal or harmful purposes, including, but not limited to:

- Users shall not develop or employ programs that harass other users. Users shall be sensitive to the public nature of shared facilities and take care not to display on screens in such locations, images, sounds or messages that could create an atmosphere of discomfort or harassment for others.
- Any intentional destruction or damage to equipment, software, or data.
- Any intentional disruption or unauthorized monitoring of electronic communications.
- SUNY Erie prohibits the use of its technology resources for any activity that violates federal, state, or local laws, or College policies. This includes, but is not limited to, the creation, possession, or distribution of pornography—especially any material involving minors, which is a federal offense. In addition, users must not engage in unauthorized access to systems (hacking), identity theft, cyberstalking, or the distribution of malicious software such as viruses, ransomware, or spyware. Use of College systems to conduct fraud, scams, or any form of criminal enterprise is strictly forbidden. SUNY Erie devices involved in such activities may be seized, and violations may result in disciplinary action and legal referral.
- Software licensed by the College must only be used in accordance with the applicable license agreements. Software is normally distributed under three kinds of licenses: proprietary, public distribution, and shareware. Unless otherwise indicated, users should assume all software made available by ITS is proprietary and may not be legally copied.
- ITS does not provide support for software that is used in violation of its license agreement. Proof of valid ownership or licensing may be required before assistance is provided.
- ITS will not knowingly allow illegally acquired software to be used on SUNY Erie-owned computers. To maintain compliance with legal and institutional standards, ITS will remove any suspect software loaded onto SUNY Erie-owned computers or servers and may do so without notice to the user.
- ITS resources (computers, equipment, network, etc.) may not be used to illegally copy, reproduce, distribute, or adapt digital media, including music files, video files, video games, software, or other copyrighted content. This prohibition includes the use of AI tools to bypass DRM or licensing restrictions, create unauthorized derivative works, or access/distribute pirated material. Violations may expose SUNY Erie to legal liability, compromise institutional integrity, and result in disciplinary action.

**Ethical Usage**

- Users must not use information technology resources, for non-college, unsanctioned, commercial activity, political advertising or campaigning. Discovery of such usage may result in disciplinary action.
- Users are prohibited from making any unauthorized attempt to alter the condition or status of any computing network component in any manner.
- Users are prohibited from making any unauthorized attempt to alter software other than their own, or to copy software intended only for execution.
- Users should not interfere with, interrupt, or obstruct the ability of others to use the network or other ITS resources.



**POLICY NAME:** Acceptable Use Policy **Continued**

- User devices in which non-owners wish to connect to must first obtain permission by the device owner.
- Users shall not provide, assist in, or gain unauthorized access to SUNY Erie computing or network resources. Discovery of such activity may result in disciplinary action.
- Users shall not attempt to circumvent or defeat computer or network security measures. Discovery of such activity may result in disciplinary action.
- Users shall not systematically collect and/or use any privately available college data or content, including users' personal directory and account information, through the use of data mining, robots, or similar gathering and extraction methods. Discovery of such activity may result in disciplinary action.

**Enforcement**

The College is the sole arbiter of what may constitute a violation of this policy. Violations of this Policy will be adjudicated, as deemed appropriate, and may include the following:

- Loss of computing privileges.
- Disconnection from the network.
- Disciplinary action.
- Prosecution under applicable civil or criminal laws.

**DOES IT SUPERCEDE A POLICY/WHICH ONE (if so, attach redline version):** Acceptable Use Policy, Board Accepted June 30, 2022.

**POLICY & GOVERNANCE COMMITTEE RECOMMENDED ACTION:**

Policy & Governance Committee recommends the Board of Trustees accept the Managerial policy under Committee Briefings, Policy and Governance Committee. This Policy supersedes all prior policies/procedures and practices related to Information Security Policy.

**DATE OF BOARD ACCEPTANCE:** January 29, 2026

**POLICY & GOVERNANCE COMMITTEE TEAM FOLLOW-UP:**

Following Trustee acceptance, this Managerial policy will be included in the SUNY Erie Community College Managerial Policy Manual.

**INFORMATION/INPUT CONSIDERED DURING POLICY & GOVERNANCE COMMITTEE DELIBERATIONS:**

1. SUNY Information Security Policy
2. SUNY Data Classification Standard
3. SUNY Cloud Security Policy



**POLICY NAME:** Acceptable Use Policy **Continued**

- 4. Acceptable Use Policy
- 5. Access Management Policy
- 6. Information Security Policy

The Policy has been reviewed and discussed at the Policy & Governance Committee meeting of January 12, 2026.

**History**

<b>Item:</b>	<b>Date:</b>	<b>Explanation:</b>
Edited Policy Adopted	January 29, 2026	
Edited Policy Adopted	June 30, 2022	
BOT Review/Revised	March 30, 2017	

**SUNY Erie Cross References**

<b>Policy Name or Procedure:</b>	<b>Where to find:</b>