SUNY SCHENECTADY COUNTY COMMUNITY COLLEGE

Facilities

Board of Trustees Policy

SUBJECT:	NUMBER:
Acceptable Use Policy - Technology	**5.6**
	DATE: **October 16, 2023** **Resolution # 23-116**
	SUPERSEDES: **June 18, 2018** **(Resolution # 18-86)**

Purpose

SUNY Schenectady (the "College") maintains technology resources in support of its educational mission and operations. This Acceptable Use Policy – Technology (this "AUP") applies to all College technology resources, including but not limited to computers, wired and wireless networking equipment, portable electronic devices, information systems, and all other electronic devices used to support the College's educational mission and operations ("College Technology Resources"). It serves as a notice to Authorized Users about permitted uses and provides a clear outline of the rules and potential consequences for violations. Authorized users include students, faculty, staff, contractors and others ("Users") approved by the College's President and/or his/her designee pursuant to procedures implemented under this AUP, as set forth in Section 9.0 below.

Policy

No Expectation of Privacy

Users have no expectation of privacy when using College Technology Resources, including but not limited to College-issued email accounts, and College-maintained computers, servers, cloud-based storage solutions, other electronic devices, and other electronic media.

All information placed on or sent using College Technology Resources may be monitored. Use of College Technology Resources constitutes consent to monitoring. Notwithstanding this Section,

private User files and email stored in individual User accounts will be accessed by the College without notice only with specific permission of the College's President, Chairperson of the Board of Trustees or Authorized Vice President. All such access will be recorded on a log, along with specific reason(s) for such access.

No Warranties

Users of College Technology Resources use those resources at their own risk. The College makes no warranties of any kind, express or implied, relating to access or use of College Technology Resources. Further, the College assumes no responsibility for the quality, availability, accuracy, nature or reliability College Technology Resources. The College is not liable for any claims, losses, damages, suits, expenses, or costs of any kind incurred, directly or indirectly, by any User through use of College Technology Resources.

Responsible Use

Use of College Technology Resources is a privilege, not a right, and access is granted with restrictions and responsibilities for acceptable use. All Users are required to conduct themselves in a responsible, decent, ethical and polite manner. Users of College Technology Resources are solely responsible for use of their account(s).

Prohibited Uses

The following uses of College Technology Resources are expressly prohibited:

- any use that violates federal, state or local laws or regulations;
- any use that violates College policies or procedures, including the Code of Conduct; and
- any use that may disrupt the College s educational mission and/or operations.

The Board of Trustees recognizes that technology changes rapidly and that it is not possible to identify each and every specific prohibited use. The College President and/or his/her designee is authorized to identify specific prohibited uses and provide notice of same to Users. Specific prohibited uses may be changed from time-to-time as necessary and appropriate.

Potentially Objectionable Content

From time to time, a User may need to access data for legitimate business and/or academic purposes that other users may find to be objectionable, including but not necessarily limited to sexually explicit images or content.

The Board of Trustees recognizes that the definition of objectionable content is subjective and that it is not possible to identify each and every specific example of potentially objectionable content. The College President and/or his/her designee is hereby authorized to identify specific potentially objectionable content and provide notice of same to Users, as necessary and appropriate.

A User must obtain permission from the College President and/or his/her designee prior to using SUNY Schenectady Computer Technology Resources to access content that has been identified as potentially objectionable.

Security Issues and Protecting Data

All Users are required to abide by the College's Information Security Policies and Procedures, including the College's Information Security Program. To protect Users, other members of the College community, the College itself and College Technology Resources from security incidents, it may be necessary to suspend or disable access to College Technology Resources without notice. It is Users' responsibility to ensure that they maintain backup and/or duplicate copies of all data stored on College Technology Resources in the event that such resources become unavailable due to security or other issues. Any backup must comply with all applicable privacy laws. No security controls are one hundred percent (100%) effective to eliminate all threats. The College is not responsible for failure of any reasonable security controls to preserve the confidentiality, integrity or availability of College Technology Resources or data stored or transmitted through College Technology Resources.

All Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of the College's proprietary information, and are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, they should consult with Information Technology Services. The user interface for information contained on Internet/Intranet/Extranet-related systems would be classified as public, internal or confidential. Examples of confidential information include but are not limited to: student information (grades, transcripts, enrollment, identification numbers, etc.) financial information, identification information of employees, and research data, etc. Users should take all necessary steps to prevent unauthorized access to this information.

Passwords are to be secure and not shared. Authorized users are responsible for the security of their passwords and accounts. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Postings using a College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the College and must be authorized by the President, unless posting is in the course of business duties.

Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Internet Access

College Technology Resources may be used to access the Internet or other remote computing resources not under the control of the College. All use of the Internet is at a User's own risk and the College has no responsibility for any content accessed through the Internet. In its sole discretion, the College may monitor data uploaded to and/or downloaded from the Internet for the purpose of (a) ensuring compliance with this and all other College policies, and (b) protecting the security of College Technology Resources, including the confidentiality, integrity and availability

of College data. Use of College Technology Resources, including any wired or wireless access points, to access the Internet constitutes consent to such monitoring.

Maintenance and Management of College Technology Resources

As the head of the Information Technology Services Department, the College's Chief Information Officer is responsible for managing College Technology Resources, including but not limited to developing appropriate procedures to implement this AUP. The College's Chief Information Officer is authorized to adopt procedures to implement the requirements of this AUP. All such procedures shall be provided to the College's President for approval prior to adoption. Board approval is not necessary for any procedure promulgated under and consistent with the requirements of this Policy.

Additional/Supplemental Policies

From time-to-time, it may be necessary or desirable to adopt additional policies relating to use, management or security of College Technology Resources. All such policies shall be in addition to and shall not replace any provision of this AUP.

Procedures

Violations of this AUP shall be reported to the Office of the President, who shall take appropriate action in accordance with this AUP and all other applicable College policies and procedures.

Penalties for students may include, but are not limited to, restriction or revocation of access privileges, suspension and other discipline consistent with all applicable College policies and procedures, including the Student Code of Conduct (Policy 3.1).

Penalties for staff and other authorized Users may include, but are not limited to, revocation of computer access privileges and other discipline allowed pursuant to contract and/or law, up to and including termination.

In addition, the College may pursue legal options for damage to College Technology Resources, or for other damages suffered by the College. Violations that appear to be criminal in nature or represent an apparent threat to any person's welfare will be reported to the appropriate law enforcement authorities.

Approved by the SUNY Schenectady Board of Trustees, October 16, 2023, Resolution # 23-116.