STATE UNIVERSITY OF NEW YORK
COLLEGE OF OPTOMETRY®

INFORMATION TECHNOLOGY SERVICES

ACCEPTABLE USE POLICY

PURPOSE

Information Technology Resources ("IT Resources") support the mission of the SUNY College of Optometry ("SUNY Optometry"), as well as all educational, instructional, clinical, research, and administrative activities. As an Authorized User of IT Resources, you have access to valuable resources and sensitive data of the College. The use of IT Resources is a revocable privilege extended to all members of the College community and it is vital for everyone to act in a responsible, ethical, honest, and legal manner when using IT Resources.

The purpose of this Policy is to outline the acceptable use of IT Resources at the College. The College is committed to ensuring open discourse and the free expression of viewpoints and beliefs. This commitment includes ensuring that academic dialogue is free from unwarranted institutional intrusion and oversight. With the values of open discourse and institutional restraint as guideposts, this Policy articulates and promotes the ethical, legal, responsible, and acceptable use of IT Resources by all members of the SUNY Optometry community and confirms the College's responsibilities in connection with accessing such information.

DEFINITION

IT Resources include, but are not limited to, computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and related materials and services.

APPLICABILITY

This Acceptable Use Policy ("Policy") applies to all Authorized Users of IT Resources at SUNY Optometry, including the SUNY College of Optometry Foundation and the Faculty Student Association of the SUNY College of Optometry. All such users, by virtue of their use of College IT Resources, agree to abide by this Policy and accept the responsibility for using such resources only for appropriate activities consistent with the College's mission. Authorized Users are responsible for reading, understanding, and behaving in a manner consistent with this Policy and other related policies pertaining to the College's IT Resources.

OWNERSHIP

The College's IT Resources are not owned by any individual or department at the College. Any IT Resources that are leased, licensed, or purchased by the College or through research contracts or grants must be administered under the terms of this Policy and the Information Security Policy for as long as they remain within the lawful possession, custody, and/or control of the College. In addition, Authorized Users must use such IT Resources in a manner consistent with U.S. Copyright law.

APPROPRIATE USE

The College's IT Resources may be used for legitimate SUNY Optometry purposes only. While the College makes IT Resources available primarily to achieve its goals of education, patient care and research, and for administrative activities, it realizes the need to permit the personal use of such resources for the convenience of the campus community.

General guidelines for acceptable use of IT Resources are based on the following principles and Authorized Users must:

- Behave responsibly and respect the name of the College and its affiliated organizations as well as the integrity and security of IT Resources and the College network at all times;
- Behave in a manner consistent with the College's mission and comply with all applicable laws, regulations, and College policies, including but not limited to appropriate College personnel policies, or Codes of Conduct;
- Be considerate and respect the rights and property of others, including privacy, confidentiality, and intellectual property (e.g., do not violate copyright laws or use software procured with academic use licenses for commercial applications or development, unless the license explicitly permits such use);
- Use computing resources for College related work in an appropriate manner (e.g., do not utilize shared resources such as CPU cycles or network bandwidth to a degree that adversely impacts academic, clinical or research activities);
- Comply with security measures employed by the College and protect your account information from unauthorized access by others; and
- Immediately report violations of this Policy to the College's Chief Information Officer or designee.

Examples of acceptable uses of IT Resources in support of or related to the College's mission include:

- Informing the College community of events sponsored by student organizations;
- Marketing or advertising of programs, classes, events, resources, or products offered or sponsored by the College or a College-related organization;
- Informing the College community of scholarships or other opportunities offered to students by third parties;
- Notifying the College community of charitable or other events.

If an Authorized User is not clear on what constitutes an appropriate use, the user should contact the Chief Information Officer or designee to determine whether a particular activity is permissible.

UNACCEPTABLE USE

Authorized Users are not permitted to:

- Engage in any activity that is illegal under local, state, federal, or international law while utilizing IT Resources. These activities include, but may not be limited to, child pornography, obscenity, harassing communications, software piracy, or threats of violence;
- Violate the rights of any party or property protected by copyright, patent, or similar laws or regulations including, but not limited to, the unauthorized sharing of educational materials by students to others without the express permission of the instructor or the College, as described in SUNY policy (*https://system.suny.edu/academic-affairs/faculty/faculty-ownership/*), unauthorized copying of copyrighted material including digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, Bit Torrent and other forms of Peer-to-Peer sharing of copyrighted information and the installation of any copyrighted software for which the College or the end user does not have an active license. *Note, however, that it is not a violation of this Policy if the unlicensed use of the copyright protected work is done in accordance with the legal doctrine of Fair Use as defined in 17 US Code Section 107 of the Copyright Act of 1976;*
- Purposefully or recklessly introduce malicious programs onto the College's network, computers, or storage areas (e.g., viruses, worms, Trojan horses, etc.) or otherwise attempt to intentionally damage, destroy, or disrupt IT Resources or the integrity of such resources or waste human or electronic resources as they relate to the College's IT Resources;

- Delete or tamper with another user's files or with information stored by another user on any information-bearing media. Even if the Authorized User's files are unprotected (with the exception of files obviously intended for public reading, such as Web pages), it is improper for another user to read them unless the owner has given permission (e.g., in an announcement in class or on a computer bulletin board);
- Reveal your College account password or any other related passwords to others or allow use of your account by others. This includes family and other household members when work is being done at home;
- Use IT Resources to actively engage in procuring or transmitting material that is in violation of sexual or gender-based harassment or hostile workplace laws:
- Use IT Resources to circulate unauthorized solicitations and advertisements for non-College related purposes, including religious and political entities and/or causes, as described in The New York State Office of Information Technology Services policy (*https://its.ny.gov/acceptable-use-information-technology-it-resources*);
- Use a wireless router, virtual private network (VPN) or other networking hardware device or networking software application installed on-site on campus that has not been authorized for use on the College Network or in conjunction with other IT Resources;
- Effect security breaches or disruptions of network communication, including wireless communication;
- Access data of which the Authorized User is not an intended recipient or log into a server or account that the Authorized User is not expressly authorized to access as a function of his/her College position. For purposes of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
- Execute any form of network monitoring tools, including packet sniffers, password capture applications, keystroke loggers, and other tools that perform similar behavior or any form of network wiretapping that will intercept data not intended for the Authorized User, unless this activity is a part of Authorized User's normal job or duty and has been approved by the Chief Information Officer or designee;
- Circumvent user authentication or security of any host, network, or account;
- Use any program, script, or command or send messages of any kind, with the intent to interfere with, or disable, a user's session; and
- Download, without consent, non-academic or non-College business related data or programs, including but not limited to freeware and shareware, unless explicitly authorized by the Chief Information Officer or designee.

Any questions you may have as to whether your use of IT Resources would violate this Policy should be brought to the attention of your supervisor or the Chief Information Officer.

CONFIDENTIALITY, PRIVACY, ACCESS, and DISCLOSURE

Authorized Users with access to IT Resources are expected to respect the privacy of the individuals whose information they access and to use reasonable and prudent methods to preserve the integrity and privacy of the accessed information to the extent possible.

Authorized Users with access to IT Resources are prohibited from using or disclosing that information for any purpose except in the course of College business with those who have a need to know, and they shall take necessary precautions to protect the confidentiality of personal information. Specific standards containing information privacy and security requirements are listed in the Information Security Policy.

Access to and utilization of IT Resources is a privilege, not a right, and the establishment of a network account does not grant or guarantee unlimited or unrestricted access. While account holders may expect reasonable access to their network accounts, this cannot be guaranteed at all times and in all circumstances. In particular, there is no guarantee of round-the-clock, seven day a week (24x7) access.

Information Technology staff routinely monitor overall system usage in order to track system problems. This involves the monitoring of overall system traffic levels and usage patterns; it generally does not involve examination of actual content.

However, under the specific written instruction of the President, the Chief Information Officer or the College's Legal Counsel, or their designee, the College may permit the inspection, monitoring, or disclosure of email and other electronically stored information, without the Authorized User's Prior consent, when:

- required by, or consistent with, applicable law, including but not limited to the New York State Freedom of Information Law, the Health Insurance Portability and Accountability Act (regarding access to health records), the Family Educational Rights and Privacy Act (regarding access to student records), and the Gramm-Leach-Bliley Act (regarding access to customer records); or any validly issued subpoena or court order;
- there is a reasonable suspicion that violations of law or College policy have occurred or may occur;
- there are time-dependent, critical operational needs of College business, if the College determines that the information sought is not more readily available by other means.

In such instances, the College will, as a courtesy, try to inform users prior to any inspection, monitoring, or disclosure of electronic records, except when such notification would be detrimental to an investigation of possible violation of law or College Policy.

Users are required to comply with college requests for access to and copies of electronic records when access or disclosure is required or allowed by applicable law or policy, regardless whether such records reside on a computer housed or owned by the College. Failure to comply with such requests can lead to disciplinary or other legal action pursuant to applicable law or policy, including but not limited to appropriate College personnel policies or Codes of Conduct.

ENFORCEMENT

The College considers violations of this Policy to be serious offenses and will take action it deems necessary to protect its network from events that threaten or degrade operations. The College reserves the right to disconnect or disable, without warning or prior notice, any computer, account, or service that poses a security or performance threat to College resources or services or that otherwise violates this or other College policies. Access may be later restored after the incident has been reviewed and the risk mitigated or eliminated. Any Authorized User found to have violated this Policy may be subject to disciplinary action, and/or the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the College or investigation and/or prosecution by the appropriate local, state, or federal authorities.

RELATED LINKS

New York State Freedom of Information Law (Article 6 of NYS Public Officers Law):
https://opengovernment.ny.gov/freedom-information-law

New York State Office of Information Technology Services –
Acceptable Use of Information Technology Resources:
https://its.ny.gov/acceptable-use-information-technology-it-resources

Health Insurance Portability and Accountability Act:
https://www.hhs.gov/hipaa/

Family Educational Rights and Privacy Act:
https://studentprivacy.ed.gov/

Gramm-Leach-Bliley Act:
https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

U.S. Copyright Office Fair Use Index:
https://www.copyright.gov/fair-use/

SUNY Policy - Copyright and Faculty Ownership of Intellectual Property:
https://system.suny.edu/academic-affairs/faculty/faculty-ownership/

RELATED POLICIES

Electronic Mail Policy
Information Security Policy

DATE	RECORD OF REVISION & CHANGES	PAGES	REVISED BY
6/30/2024	Original Document		RP/WLR