

SUNY College at Oneonta Information Technology Acceptable Use Policy

Policy Statement

The College's Information Technology resources are intended for the exclusive use of people having a relationship with the College who have been assigned a valid user account. College information technology facilities are a valuable resource for College use, and they should be conserved. This policy defines acceptable use of the College's Information Technology resources, both physical (computers, networks, etc.) and informational (passwords, data, software, etc.).

Rationale

Information and access to it is essential to the educational mission and the business processes of the College. Information Technology must be used in a way that does not unreasonably compromise users' privacy, the security of information or availability of resources to support the work of the College community.

Applicability of the Policy

This policy applies to anyone who uses any of the College's Information Technology resources.

Policy Elaboration

Individual Accountability

Use of Information Technology resources by an individual will be granted through an assigned user account or accounts. Usernames and passwords will be issued to employees and students through the Account Creation process or other processes as required. Access for others will be granted through the Sponsored Account process or other processes as required. Acceptance of this policy is required to obtain an account and access to Information Technology Resources.

Oneonta passwords must not be shared and must be protected from malicious use. The user is responsible for any activity related to their accounts.

Changing another person's password or representing another person without their authority is prohibited.

A specific individual will always be responsible for activity in any cooperative account, such as club or departmental accounts.

Users are responsible for their use of Information Technology resources including accounts and usernames. The following uses are not permitted based on the New York State Information Technology Policy IT Best Practice Guideline:

- Writing personal communications in a manner that could reasonably be interpreted as official State or SUNY Oneonta policies,
- Conducting of outside employment or self-employment activities or private marketing or private advertising of products or services not related to College activities,
- Engagement in political activity,
- Soliciting for or promoting any not-for-profit, religious, political or personal causes, except in cases where the College has endorsed such activity.
- Obtaining personal services, including but not limited to dating or social network sites for personal use(ex. Using a College assigned email account to sign up for a personal Facebook site), except in the case of students

SUNY College at Oneonta Information Technology Acceptable Use Policy

- Mass distribution of any communication, including “chain” letters, except as permitted in SUNY Oneonta’s Broadcast Email Policy,

Transmitting rude, obscene or harassing material via any electronic facility provided by the College could be considered harassment. Users should take care to avoid sending, forwarding or otherwise transmitting material that may be considered harassing. Users should be aware that federal Telecommunications legislation specifies penalties for harassment, the transmission of indecent material and for the transmission of indecent material to people, or available to people, under 18 years of age even at their request. Inappropriate display of offensive material may be considered harassment.

Unauthorized Use

Unauthorized access to restricted databases, servers or networks is prohibited and will be considered a violation of this Policy. Addition of a server or any other device on any of the SUNY networks must be authorized by the departments of technology services.

Users must not browse, access, copy or change other users’ files, nor change public files without authorization.

Users must not attempt to modify any computer system or software in any unauthorized manner. The use of malicious software, such as "worms" and "viruses" destructive to computer systems, is illegal. Users are prohibited from circumventing, probing or scanning security measures unless such activity is included in their job duties.

Copyright

Users should be aware that information content may be protected by copyright laws. Ownership of information should be considered prior to use. Users of the College’s Information Technology resources should be aware of their responsibilities under intellectual property laws including United States Copyright Law and the Digital Millennium Copyright Act.

Copyrighted software must only be used in accordance with its license or purchase agreement. Users do not have the right to receive and/or use unauthorized copies of software, or make unauthorized copies of software for themselves or others.

Personal Use

Personal use should be subordinate and subject to the educational and business needs of the College and not interfere with the conduct of the College’s business. Personal use should not interfere or disrupt in any way other users, SUNY Oneonta’s Information Technology systems, network users, services or equipment.

Personal Use by Non Students

Personal use of SUNY Oneonta’s Information Technology systems should be limited and consistent with the requirements of Executive Order No. 7 (concerning personal use of State Property). Where personal use of such Information Technology systems has been granted, such use should be permitted only with the restrictions outlined below.

SUNY College at Oneonta Information Technology Acceptable Use Policy

Personal use should only account for an incidental amount of a user's time. Personal use is restricted to College employees and is not extended to the employee's family members or acquaintances.

Personal Use by Students

Personal and recreational use of the College's Information Technology resources is permitted for students. Recreational use such as game playing, the use of social media, and the viewing of online television and videos must not impede academic uses.

Sanctions

Violations of this Policy for the Use of Campus Information Technology are treated like other academic dishonesty or misuse of property violations consistent with Federal, State, SUNY and College policies. Violators may also be billed for illegal use of the computer systems and may be prosecuted for statutory violations.

User Expectations

The College will make every effort to ensure but cannot completely guarantee the privacy of e-mail because of the nature and technology of electronic communication. That is, users should expect that e-mail may be insecure because of external factors such as lost or stolen passwords and computer "hacking." Confidential or personally identifiable information should only be transmitted in the most secure manner available.

Users should be aware that the College's backup files may contain copies of e-mail messages and electronic files even if those e-mail messages or files have been deleted from the users' accounts and network drives.

Though e-mail messages, electronic files and network use are not routinely monitored, the College does maintain the right, as owner of the campus network and servers, to review, monitor or forward them.

Permission to monitor or review e-mail or electronic files or network activity under the following circumstances may be granted by the College President or his/her designee:

- Abuse has been reported and must be investigated,
- There is an imminent risk to health or safety,
- Investigations into inappropriate activity related to an individual's employment or studies,
- The College is legally required to do so.

Permission to monitor or review e-mail or electronic files under the following circumstances may be granted by the Information Security Officer or his/her designee.:

- The College has a legitimate business purpose to do so (such as following the termination or extended absence of an employee),
- It is required to diagnose and resolve technical problems.

SUNY College at Oneonta Information Technology Acceptable Use Policy

When the owner of the account is no longer associated with the College or its affiliated parties, the College also maintains the right to review or forward e-mail messages and other electronic files in cases where the data contained is pertinent to the business of the College. In such cases, the direct supervisor of the account owner may contact the College ISO or his/her designee who will work with the supervisor to determine which files are pertinent and copy or forward those files to a location accessible by the supervisor or his/her designees. No other files will be copied and original files associated with the account will not be moved, deleted or altered. The original files and accounts will be disabled and deleted in accordance with established College policies.

Definitions

Information Security Officer – Designated by the President, the Information Security Officer (ISO) is responsible for overseeing Oneonta's IT Security environment. See Section 2 of [SUNY Oneonta's Information Technology Security Program](#).

Information Technology resources - Computers, notebook computers, mobile devices, servers, computer networks, network connections, modem connections and any other device that involves computing and/or network connectivity. It also applies to computer files, programs, or data stored on floppy disk, hard disk, magnetic tape, CD-ROM, cartridge, removable hard drives, zip drives, flash drives, network storage or any other digital storage media

Username - An individually assigned unique computer identifier. Also known as usercode or user-id

User Account – Any account assigned to an individual to provide access to various IT resources. Common accounts include domain accounts providing, among other things, login to computers; email accounts; Banner or Webservices accounts; and Angel Course Management accounts.

Contacts

Questions related to the daily operational interpretation of this policy should be directed to:

Todd Foreman, Vice President for Finance and Administration
607-436-2081
forematd@oneonta.edu

Related Documents / Policies

<http://policies.oneonta.edu/PDF/Information%20Technology%20Security%20Program-0034-20091210-1257.pdf>

Broadcast Email Policy

<http://policies.oneonta.edu/PDF/BroadcastE-mailPolicy-84-20100114.pdf>

NYS Information Security Policy

<http://www.dhss.ny.gov/ocs/resources/documents/Cyber-Security-Policy-P03-002-V3.4.pdf>

The Digital Millennium Copyright Act Of 1998

<http://www.copyright.gov/legislation/dmca.pdf>

IT Best Practice Guideline: Acceptable Use of Information Technology (IT) Resources

<http://cio.ny.gov/policy/NYS-P09-002.pdf>

Copyright

<http://www.copyright.gov/>

SUNY College at Oneonta Information Technology Acceptable Use Policy

Effective Dates

- Approved by Cabinet on April 4, 1999
- Revised by Cabinet on February 1, 2011