



Responsible Use of COTC Computing and Network Resources Policy 1.1.3

College Policy

Applies to: Faculty, staff, student employees, students and any other person using college-owned computing resources

Responsible Office

The Office of the President

POLICY STATEMENT

This policy provides guidance for establishing responsibilities and limitations associated with the use of college computing resources. The general guiding principle behind the policy is that “cyberspace is not a separate jurisdiction;” that applicable laws, rules, and policies apply equally to the use of college computing resources.

Adherence to this policy will require compliance with all applicable laws and college policies, and all applicable restrictions whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

Purpose of the Policy

To provide expectations to support the responsible use of college computing resources.

Definitions

Term	Definition
Computing resources	Computers, computer systems, networks, and devices including by not limited to mobile phones, smartphones, and other mobile devices, and the institutional data that they contain.
The Office of the Chief Information Officer (OCIO), The Ohio State University	The OCIO provides Information Technology (IT) services to Central Ohio Technical College (COTC).

Policy Details

- I. As a part of the physical, social and educational learning infrastructure that is in-place for the Central Ohio Technical College (COTC) Newark and extended campuses, COTC acquires, develops, and maintains computers, software, computer systems, and networks. These **computing resources** are intended to support COTC's academic mission, including direct and indirect support of COTC's mission and student life activities. In addition, these computing resources support all administrative staff functions required to operate the college. Furthermore, these computing resources are used to support the free exchange of ideas among members of the COTC community, and between the COTC community and the wider communities with which the college interacts.
- II. The rights of academic freedom and freedom of expression apply to the use of COTC's computing resources. However, there are acceptable social and ethical responsibilities/limitations associated with those rights. The use of COTC computing resources, like the use of any other COTC provided resource or related activity, is subject to the normal requirements of legal, regulatory, and ethical behavior based on the values that we hold as a public higher education institution. Responsible use of a computing resource does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable guidelines contained in this policy, whether or not they are built into the operating system or network, and whether or not they can be circumvented by technical means.

Responsible Use of COTC Computing and Network Resources

Policy 1.1.3

College Policy

Applies to: Faculty, staff, student employees, students and any other person using college-owned computing resources

- III. This policy covers the use of college computing and network resources, regardless of location or device.
- IV. Additional policies may apply, refer to the Information Technology (IT) policy area on the COTC website and the Resource section of this document for further information.

PROCEDURE

- I. All users of COTC computer resources must:
 - A. **Comply with all federal, Ohio, and other applicable law; all generally applicable COTC rules, policies and other governing documents; and all applicable contracts and licenses.**
 - 1. Examples of such laws, rules, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking" and similar activities; COTC's Code of Student Conduct; COTC's Privacy and Release of Student Education Records Policy; COTC's Sexual Misconduct, Sexual Harassment and Relationship Violence Policy; the Agreement Between Central Ohio Technical College and The United Faculty/Central Ohio Technical College, AFT/OFT; and all applicable software licensing agreements.
 - 2. Users who engage in electronic communications with persons in other states or countries, or on other systems or networks should be aware that they also may be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular use cases.
 - B. **Use only those computing resources they are authorized to use and use them only in the manner and to the extent authorized.** Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
 - C. **Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.** Ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
 - D. **Respect the finite capacity of COTC's computing resources and limit use so as not to consume an unreasonable amount of resources or interfere unreasonably with the activity of other users.** COTC may impose limitations applicable to use of available COTC computing resources. The reasonableness of any particular use will be judged in the context of all the relevant circumstances.
 - E. **Refrain from Unauthorized Peer-to-Peer File Sharing.** Peer-to-Peer (P2P) file sharing refers to the distribution and sharing of digital media content such as books, music, movies, and games. The use of COTC provided computing resources for the purpose of downloading this content is unauthorized unless specifically approved ahead of time by the instructor and the OCIO. It will only be approved if needed for the completion of instructional assignments or projects that are part of the curriculum offered by COTC.

Responsible Use of COTC Computing and Network Resources

Policy 1.1.3

College Policy

Applies to: Faculty, staff, student employees, students and any other person using college-owned computing resources

- F. **Refrain from using COTC provided computing resources for personal commercial purposes or for personal financial or other gain.** Personal use of COTC computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other COTC responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures, or as a matter of unit policy.
- G. **Refrain from stating or implying that you speak on behalf of COTC and from using COTC trademarks and logos without authorization to do so.** Affiliation with COTC does not, by itself, imply authorization to speak on behalf of COTC. This also extends to the use of social media. Authorization to use COTC trademarks and logos on COTC computing resources will be done in accordance with guidelines provided by the Marketing and Public Relations Department (MPR). Contact MPR for further information and authorization.
- H. **Refrain from using campus computing resources to access, transmit, copy or save pornographic, obscene, indecent, lewd or lascivious material or material that panders to bigotry, sexism, or other forms of discrimination.**

II. Security and Privacy

- A. COTC employs various measures to protect the security of its computing resources and users' accounts. Users should be aware that COTC cannot guarantee such security. Users should engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and regularly changing them. Accounts and passwords may not be shared with, or used by, persons other than those to whom they have been assigned by the college.
- B. While COTC does not routinely monitor individual usage of its computing resources, the college may specifically monitor the activity and access the accounts of individual users of college computing resources, including individual login sessions and communications without notice, when:
 - 1. The user has given permission or has voluntarily made them accessible to the public, for example by posting to a publicly-accessible web page or providing publicly-accessible network services.
 - 2. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the institutions computing resources or to protect COTC from liability.
 - 3. There is reasonable cause to believe that the user has violated, or is violating, this policy
 - 4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the reviewing of general activity and usage patterns.
 - 5. Access is necessary and conducted pursuant to applicable college rules, policies and procedures.
 - 6. It is otherwise required or permitted by law.

Any such individual monitoring, other than that specified above, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the president and a representative from the OCIO.

- C. Users also are advised that their use of COTC computing resources is not completely private. For example, the normal operation and maintenance of the college's computing resources requires the

Responsible Use of COTC Computing and Network Resources Policy 1.1.3

College Policy

Applies to: Faculty, staff, student employees, students and any other person using college-owned computing resources

backup and caching of data and communications, logging of activity, reviewing the general usage patterns for the unauthorized disclosure of institutional data, scanning of systems and network ports for anomalies and vulnerabilities, and other such activities that are necessary to render service or to meet college legal obligations.

- D. COTC, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate COTC personnel or law enforcement agencies and may use those results in appropriate COTC disciplinary proceedings. Communications made by means of college computing resources are subject to Ohio’s Public Records Act the same as any other record.

III. Enforcement

- A. Users who violate this policy may be denied access to COTC computing resources and may be subject to other penalties and disciplinary action, both within and outside of COTC. Violations will normally be handled through COTC disciplinary procedures applicable to the relevant user.
- B. COTC may temporarily suspend or block access to an account, prior to the initiation or completion of such disciplinary procedures, when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of COTC or other computing resources, or to protect COTC from liability. COTC may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Responsibilities

Position or Office	Responsibilities
Office of the Chief Information Officer, The Ohio State University	<ol style="list-style-type: none"> 1) Ensure appropriate practices as to usage of computing devices is supported and maintained 2) Report any violations of this policy to appropriate executive management 3) Manage policy inquiries 4) Manage policy enforcement 5) Coordinate prior authorization for investigative monitoring
Users of Computing Resources	<ol style="list-style-type: none"> 1) Ascertain, understand, and comply with applicable laws; this policy, college rules, policies, and other governing documents; contracts; and licenses. 2) Use only those computing resources you are authorized to use and only in the manner and extent authorized. 3) Respect the privacy of other users and their accounts. 4) Limit use so as not to interfere unreasonably with the activities of other users. 5) Refrain from using college resources for personal commercial purposes or for personal financial or other gain.
The Office of Human Resources	<ol style="list-style-type: none"> 1) Provide guidance related to disciplinary proceedings in accordance with applicable Human Resources policies. 2) Conduct fact-finding investigations and issue findings and action steps regarding employee allegations of policy violations. 3) Issue corrective action as appropriate
Dean of Students	<ol style="list-style-type: none"> 1) Investigate alleged policy violations by students 2) Impose any penalties or other disciplinary measures

Resources

- Agreement Between Central Ohio Technical College and The United Faculty/Central Ohio Technical College, AFT/OFT.



Responsible Use of COTC Computing and Network Resources Policy 1.1.3

College Policy

Applies to: Faculty, staff, student employees, students and any other person using college-owned computing resources

- [Code of Student Conduct](#)
- Ohio Ethics Policy 2.1.35
- Privacy and Release of Student Education Records Policy 5.1.20
- [Sexual Misconduct, Sexual Harassment and Relationship Violence](#) Policy 2.1.20

Contacts

Subject	Office	Telephone	E-mail/URL
Policy questions, authorization for investigatory monitoring	Office of the Chief Information Officer, The Ohio State University	740-366-9244	nwk-helpdesk@osu.edu
Corrective Action	Office of Human Resources	740-366-9367	Henderson.385@mail.cotc.edu
Student Enforcement	Office of Student Life	740-364-9578	Mason.536@mail.cotc.edu

History

Issued: 05/10/2000
Revised: 09/13/2011
Revised: 02/12/2021