Information Technology and Resources

Acceptable Use of Technology

Overview

Acceptable Use standards define what users may or may not do in the process of utilizing Cincinnati State information technology (IT) resources.

Scope

This standard addresses the use of Cincinnati State communications services and the communication of information among Cincinnati State employees (full-time and part-time), students, contractors, and vendors.

Cincinnati State reserves the right to modify this standard from time to time at its discretion.

Introduction

This policy contains the College’s philosophy, policy, rules, and standards regulating the use of technology resources. It is the responsibility of all students and all who are employed by the College, whether they are employed as students, temporary personnel, contractors, consultants, staff, or faculty, to implement and comply with this policy and all other applicable regulations and to maintain the highest standard of ethics when dealing with information technology resources.

General Statement

In support of its mission of teaching and community service, Cincinnati State Technical and Community College acquires, develops, maintains, and provides access to information technology and resources for students, temporary personnel, contractors, consultants, faculty, and staff. These resources include but are not limited to telecommunications systems (land lines, facsimile machines), computers, laptops, cell phones, computer terminals, peripheral computer hardware, software, networks (wired and wireless), and the information that can be accessed using these tools. These computing resources are intended for College-related use, including direct and indirect support of the College's instruction, research, and service missions; College administrative functions; student and campus life activities; and the free exchange of ideas.

The rights of free expression and academic freedom apply to the use of College computing resources. So, too, however, do the responsibilities and limits associated with those rights. All who use the College's computing resources must act responsibly, in accordance with the highest standard of ethical and legal behavior. Thus, legitimate use of computing resources does not extend to whatever is technically possible. Users must abide by all applicable restrictions, whether or not they are built into the client device, operating system, application software, or network and whether or not they can be circumvented by technical means.

This policy applies to all users of College computing resources, whether affiliated with the College or not, and whether the users access resources from on campus or remote locations. This policy applies equally to College-owned or College-leased technology resources. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of the College or to uses within specific units.

Policy

All College computing resource users must:

1. Comply with all federal, Ohio, and other applicable law; all generally applicable College rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, polices, contracts, and licenses include: the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Family Educational Rights and Privacy Act (FERPA); the Health Insurance Portability and Accountability Act (HIPAA); the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; the College's Student Code of Conduct; the Cincinnati State Technical and Community College Operations Manual, faculty handbooks, and the College's sexual harassment policy; and all applicable software licenses. Users must respect copyrights, intellectual-property rights, and ownership of files and passwords. Unauthorized copying of files or passwords belonging to others or to the College may constitute plagiarism or theft. Accessing or modifying files without authorization (including altering information, introducing viruses or Trojan horses, or damaging files) is unethical, may be illegal, and may lead to sanctions. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also 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 uses. Cincinnati State extends these policies and guidelines to systems outside the College that are accessed via the College's facilities (e.g., electronic mail or remote logins using the College's Internet connections).
2. Use only those computing resources that 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. Accounts, passwords, and other authentication mechanisms, may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the College.
3. Respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of College computing resources, the College may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.
4. Limit the personal use of College computing resources and refrain from using those resources for personal commercial purposes or for personal financial or other gain. Personal use of College computing resources is permitted on a limited basis when it does not interfere with the performance of the user's job

or other College responsibilities, and is otherwise in compliance with this and other College policy. College computing resources are not to be used for commercial purposes without written authorization from the College. In such cases, the College may require payment of appropriate fees. This usage does not include links to personal web pages. This usage is subject to monitoring by the ITS staff. Further limits may be imposed upon personal use in accordance with normal supervisory procedures. Any personal use of computing resources that disrupts or interferes with College business, incurs an undue cost to the College, could potentially embarrass or harm the College, or has the appearance of impropriety is strictly prohibited. Personal use that is strictly prohibited includes, but is not limited to, the following:

a. Violation of Law. Violating or supporting and encouraging the violation of local, state, or federal law is strictly prohibited.
b. Illegal Copying. Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music, and graphics in violation of copyright laws is strictly prohibited.
c. Operating a Business. Operating a business, directly or indirectly, for personal gain is strictly prohibited.
d. Accessing Personals Services. Accessing or participating in any type of personals ads or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or personals ads is strictly prohibited.
e. Accessing Sexually Explicit Material. Downloading, displaying, transmitting, duplicating, storing, or printing sexually explicit material is strictly prohibited.
f. Harassment. Downloading, displaying, transmitting, duplicating, storing, or printing material that is offensive, obscene, threatening, or harassing is strictly prohibited.
g. Gambling or Wagering. Organizing, wagering on, participating in, or observing any type of gambling event or activity is strictly prohibited.
h. Mass E-mailing. Sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters in bulk to recipients inside or outside the state environment is strictly prohibited.
i. Solicitation. Except for agency-approved efforts, soliciting for money or support on behalf of charities, religious entities, or political causes is strictly prohibited.
j. Damage or Theft. Any attempt by users to damage or disrupt the operation of computing equipment, communications equipment, or communications lines; or attempting to remove College owned or leased equipment without written approval of the Chief Information Officer (CIO) is strictly prohibited and will be subject to disciplinary action.
k. Participation in Online Communities. Any use of state-provided IT resources to operate, participate in, or contribute to an online community including, but not limited to, online forums, chat rooms, listservs, blogs, wikis, peer-to-peer file sharing, and social networks, is strictly prohibited unless organized or approved by the agency.
l. Internet Security. A public servant participating in an online community organized or approved by the agency shall adhere to the security requirements and policies of the College.
m. Unauthorized Installation or Use of Software. Installing, copying, or using software including, but not limited to, instant messaging clients and peer-to-peer file sharing software, or personally-owned software, without the approval of the CIO is strictly prohibited. Installation and use of unlicensed software is strictly prohibited.

5. Refrain from stating or implying that they speak on behalf of the College and from using College trademarks and logos without authorization to do so. Affiliation with the College does not, by itself, imply authorization to speak on behalf of the College. Authorization to use College trademarks and logos may be granted only by Cincinnati State. The use of appropriate disclaimers is encouraged. Personal web pages linked to the College website should disclaim association with Cincinnati State.
6. Respect that there is no expectation of privacy. This policy serves as notice to users that they shall have no reasonable expectation of privacy in conjunction with their use of College provided IT resources. Contents of College computers may be subject to review, investigation, and public disclosure. Access and use of the internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by state or federal law. The College reserves the right to view any files and electronic communications on state college computers, monitor and log all electronic activities, and report findings to appropriate supervisors and authorities.

While the College does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of College computing resources requires the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service.

The College may also monitor the activity and accounts of individual users of College computing resources, including individual sessions and communications, without notice. This may occur:

a. when the user has voluntarily made them accessible to the public, as by posting to Usenet or a website;

b. when it reasonably appears necessary to do so to protect the integrity, security, or functionality of College or other computing resources or to protect the College from liability;

c. when there is reasonable cause to believe that the user has violated, or is violating, this policy;

d. when an account or device appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or

e. when it is otherwise required or permitted by law

Any such individual monitoring, other than that specified in (a) above, or required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer (CIO) or his/her designee.

The College, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate College personnel or law enforcement agencies and may use those results in appropriate College disciplinary proceedings

Impeding Access: Impeding the College's ability to access, inspect, and monitor IT resources is strictly prohibited. A user shall not encrypt or conceal the contents of any file or electronic communications on College computers without proper authorization. A user shall not set or manipulate a password on any College computer, program, file, or electronic communication without proper authorization.

Misrepresentation: Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible, or offensive behavior in electronic communications is strictly prohibited.

Protection of College Data

Users of College information resources—especially faculty and staff—have a responsibility to protect sensitive information. This includes but is not limited to student and employee personal information and College financial data. All users are expected to report suspected or discovered security incidents, such as social engineering and virus attacks.

Privacy and Security

Information technology provides important means of communication, both public and private. Users and system administrators must respect the privacy of person-to-person communication in all forms, including voice (telephone), text (electronic mail and file transfer), and image (graphics and television). The principle of freedom of speech will apply to public communications in all these forms.

The College employs various measures to protect the security of its computing resources and users accounts. However, users should be aware that the College does not and cannot guarantee such security.

Any use of College-provided IT resources that interferes with or compromises the security or operations of any computer system, or compromises public trust, is strictly prohibited. Privacy and security violations can be, but are not limited to the following:

- Confidentiality Procedures. Using IT resources to violate or attempt to circumvent confidentiality procedures is strictly prohibited.
- Accessing or Disseminating Confidential Information. Accessing or disseminating confidential information or information about another person without authorization is strictly prohibited.
- Accessing Systems without Authorization. Accessing networks, files or systems or an account of another person without proper authorization is strictly prohibited.
- Disclosing Passwords: Users are individually responsible for safeguarding their passwords, which means they are not to disclose them to another user.
- Distributing Malicious Code. Distributing malicious code or circumventing malicious code security is strictly prohibited.

Enforcement of this Policy

The College demands a high standard of conduct for all students, faculty, and staff in the use of, and access to the College's information technology and resources. Anyone whose conduct misuses the College's information technology and resources is subject to College disciplinary action. This conduct includes, but is not limited to, the aforementioned policies and security and privacy concerns.

Alleged violations of this policy shall be dealt with in accordance with the procedures in the Cincinnati State Technical and Community College personnel policies described in the College Operations Manual, College collective bargaining agreements, and the Student Code of Conduct. The College treats violations of this policy seriously and will pursue criminal and civil prosecution where appropriate.

Whenever it becomes necessary to enforce College rules or policies, an authorized administrator may: disallow network connections by certain computers (even departmental and personal ones); require adequate identification of computers and users on the network; undertake audits of software or information on shared systems where policy violations are possible; take steps to secure compromised computers that are connected to the network; or deny access to computers, the network, and institutional software and databases.

Sanctions Regarding Misuse of Computing Resources Content

Users who violate this policy may be denied access to College computing resources and may be subject to other penalties and disciplinary action, both within and outside of the College. Violations will normally be handled through the College disciplinary procedures applicable to the relevant user. Alleged violations by students normally will be investigated, and the appropriate administrative office will normally impose any penalties or other discipline.

However, the College, through its information managers, may suspend or block access to an account prior to the initiation or completion of such procedures when it reasonably appears necessary to do so, and in order to protect the integrity, security, or functionality of College or other computing resources, or to protect the College from liability.

Resources

This policy conforms to Ohio IT Policy ITP-E.8 "Use of E-mail, Internet and Other IT Resources."

Student Recording and Distribution of Course Lectures and Materials

Students may not photograph, record (using audio or video technology), duplicate, reproduce, transmit, distribute, or upload or share via internet or website environments any class lectures, discussion, and/or other course materials, unless written permission has been obtained in advance from the instructor.

In the case of class discussions and/or presentations, permission must also be obtained from all students in the class and any guest speakers, if applicable. All participants must be informed in advance that activities will be recorded.

Students should review the course syllabus for instructions regarding the instructor's policy on class recordings. Unless directly authorized by the syllabus, any student wishing to record classroom activities must discuss this issue with the instructor and obtain written permission.

Any photograph or recording of class activities and/or materials is authorized solely for use as an educational resource by an individual student or, when permission is granted, with other students enrolled in the same class. Photographs and/or recordings may not be publicly exchanged, distributed, shared, or broadcast for any purpose.

Permission to allow a photograph or recording is not a transfer of any copyrights.

Violation of this policy may subject a student to disciplinary action under the College's Student Code of Conduct (http://catalog.cincinnatistate.edu/archives/2020-2021/studentrightsandresponsibilities/studentresponsibilities/).

Exception: it is not a violation of this policy for a student determined by the Office of Disability Services to be entitled to educational accommodations to exercise any rights protected under Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990, including needed recording or adaptations of classroom lectures, discussions, and/or course materials for personal research and study. However, all other restrictions on other use and/or distribution apply in such cases.