Information Technology and Resources

Responsible Use of Information Technology and Resources

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.

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

General Statement: In support of its mission of teaching and community service, Cincinnati State acquires, develops, maintains, and provides access to information technology and resources for students, temporary personnel, contractors, consultants, faculty, and staff. These resources include telecommunications systems, computers, laptops, PDA's, computer terminals, peripheral computer hardware, software, networks, and the information that can be accessed using these tools. These computing resources are intended for College-related use 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:

- Comply with all federal, Ohio and other applicable laws; 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 code of student conduct; the Cincinnati State Technical and Community College Administrators' Manual, Faculty Handbook, the College's sexual harassment policy; and all applicable software licenses.
- Respect copyrights, intellectual-property rights, 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).
- 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.
- 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.
- 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:

- Violation of law: Violating or supporting and encouraging the violation of local, state or federal law is strictly prohibited.
- 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.
- Operating a business: Operating a business, directly or indirectly, for personal gain is strictly prohibited.
- 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.
- Accessing sexually explicit material: Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material is strictly prohibited.
- Harassment: Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening or harassing is strictly prohibited.
- Gambling or wagering: Organizing, wagering on, participating in or observing any type of gambling event or activity is strictly prohibited.
- 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.
- Solicitation: Except for agency-approved efforts, soliciting for money or support on behalf of charities, religious entities or political causes is strictly prohibited.
- 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 Chief Information Officer (CIO) is strictly prohibited and will be subject to disciplinary action.
- 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.
- Internet security: A public servant participating in an online community organized or approved by the agency shall adhere to the security requirements and policies by the College.
- 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.
- Copying College-owned or licensed software or data for personal or external use without prior written approval; or attempting to modify or copy College-owned or another users licensed software or data without prior approval is strictly prohibited.
- Unauthorized installation or use of hardware: Installing, attaching, or physically or wirelessly connecting any kind of hardware device to any state-provided IT resource, including computers and network services, without prior authorization is strictly prohibited.

- 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.
- 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:
- When the user has voluntarily made them accessible to the public, as by posting to Usenet or a website;
- 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;
- When there is reasonable cause to believe that the user has violated, or is violating, this policy;
- 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
- When it is otherwise required or permitted by law.

Any such individual monitoring, other than when a user has voluntarily made activity publicly accessible, or is required by law or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer (CIO) or a designee of same. 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 state 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. 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 following policies and security and privacy issues.

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 Employee Handbook, Administrator's 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: 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 will normally be investigated, and the Student Services 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.

Peer to Peer File Sharing Policy

Overview. Peer-to-Peer (P2P) applications have become the most popular and controversial method through which digital files of various formats and types are traded, shared, and distributed across the Internet. While Cincinnati State Technical and Community College recognizes that there are legitimate uses for P2P applications, the College also understands that significant risks are implicit in the use of such applications.

The College does not seek to ban P2P file sharing from the campus network, and will continue to support academic freedom and any technologies that can be used to foster collaboration. However, Cincinnati State must also protect its assets, its reputation, and its resources. This policy has been implemented in order to mitigate exposure of Cincinnati State Technical and Community College to security risks and liabilities associated with the irresponsible use of P2P applications on College resources.

Scope. This policy shall apply to all computer workstations, laptops, servers, networked appliances, and any other device capable of participating in a P2P network if such device is owned by Cincinnati State; or any device utilizing College network resources, even if that device is owned privately or

by a third party. This policy applies to faculty, staff, students, contractors, consultants, temporaries, and other workers at Cincinnati State, including all personnel affiliated with third parties at such time they are using any resource described above.

Prohibited Activity. This policy strictly prohibits the distribution, downloading, uploading, or sharing of any material, software, data, document, sound, picture, or any other file that is:

- Specified as illegal by any federal or state law, statute, proclamation, order, or decree.
- Copyrighted and not authorized for distribution by the copyright owner.
- Considered to be proprietary, privileged, private, or otherwise vital to the operation of the College; including, but not limited to, personnel, student, financial, or strategic records and documents, or any material governed by federal and state regulations.
- Any virus or malware for the purpose of deployment or implementation with ill-intent.

Any P2P activity is strictly forbidden in the cases of:

- Computer labs
- Computer workstations and other network devices readily accessible to multiple users.
- Computer workstations and other network devices used in daily operation by areas and departments heavily affected by federally mandated regulatory compliance.
- Laptops, computer workstations, and any other network capable device provided by Information Technology through equipment services.

Users of Cincinnati State resources may not attempt to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by the College for the purpose of P2P mitigation.

Rights and Responsibilities. Students, faculty, staff, contractors, consultants, temporaries, and other workers at Cincinnati State shall bear legal/financial responsibility for events resulting from their own use of P2P applications. Individual departments, colleges, administrative areas, and other entities must respond in a timely and efficient manner to all inquiries and complaints that arise in regard to this policy.

Information Technology and Cincinnati State are required by federal law to report certain illegal activities to specified law enforcement agencies without notice to the user or the appropriate department.

College students are particularly vulnerable to the watchful eyes of the RIAA (Recording Industry Association of America) and the MPAA (Motion Picture Association of America). Copyright holders contact Cincinnati State on a regular basis demanding that the illegal distribution of their material be stopped.

Technology Mitigation. Information Technology will implement and maintain a network appliance specifically designed to control and track P2P usage. This technology called CopySense, by Audible Magic Corp can identify and block illegal sharing of copyrighted files while allowing other legitimate peer-to-peer uses to continue.

P2P traffic will be limited in bandwidth, to ensure that network resources are available for all business- and education-related needs and processes.

P2P traffic may be blocked for specific areas described under this policy. Outbound P2P traffic positively identified as copyrighted material will be blocked. CopySense filters copyrighted peer-to-peer content by sensing an electronic fingerprint unique to the content itself. When a computer is found using software to obtain copyrighted material in violation of the DMCA, the computer network access will be suspended without notice.

P2P traffic and usage information will be collected, and the collected information will be governed by the policies set forth in section five of this document.

Privacy. Logs detailing P2P traffic and usage on the Cincinnati State network will be collected. Logs will contain IP addresses involved in data transfer, direction of transfer (if retrievable), metadata of file (if retrievable), time, protocol used, and amount of data transferred. Logs will not contain any personal identifying information. Logs will be kept for six weeks (42 days).

Logs will be subject to periodic review for enforcement of this policy. Information collected may be used in aggregate format for reporting purposes. Individual usage will not be actively or routinely monitored. Logs maybe used to investigate complaints or suspicious traffic patterns.

Individual divisions, departments, functional or administrative areas, and entities of Cincinnati State may request information about P2P usage pertinent to that area. This request may only be made by the dean, chair, department head, manager, or other leadership of the area requesting information.

Information Technology will not release any information collected by the appliance to any entity external to Cincinnati State unless compelled or obligated by law or court order, subpoena, warrant, or writ; with the exception of Audible Magic Corporation, which will receive data exclusively in aggregate format, with no personal identifying information, for purposes of internal statistical analysis.

Enforcement. Any faculty, staff, or student found to have violated this policy may be subject to disciplinary action, up to and including suspension, expulsion, and/or termination of employment in accordance with procedures defined by Cincinnati State administrative policies stated in the handbook governing that individual, criminal and/or civil prosecution.

Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract, criminal and/or civil prosecution.

Definitions. P2P, in the context of this policy, is defined as direct data communication between two or more network capable devices over the Internet or other network, usually for the purpose of sharing any data file (including, but not limited to: music, pictures, video, software, and documents). Here are definitions for other terms discussed in this document:

- P2P network, in the context of this policy, is defined as a collection of distributed network-capable devices participating in P2P activity.
- P2P application is defined as any application that allows a network-capable device to participate in one or more P2P networks.
- Sharing, in the context of this policy, describes the action and activity of making any data file available to one or more P2P networks.
- Logs are defined as collections of information, typically used to document activity and events.
- Uploading describes network trafficking of data files originating from the Cincinnati State network and destined for an external network.
- Downloading describes network trafficking of data files originating from an external network and destined for the Cincinnati State network.
- The Cincinnati State network and networking resources describe all materials and devices owned by the Cincinnati State Technical and Community College and used to provide network connectivity to any network capable device. This includes all jacks, cable, hubs, wireless access points, switches, and routers.

The Digital Millennium Copyright Act (1998), DMCA, seeks to protect copyright holders from the technological circumvention of previous copyright statues. In 1976 the concept of “Fair Use” was added to the existing copyright clause of the US Constitution. Fair Use is not defined in the constitution; it was decided in the courts. There are, however, Supreme Court decisions that have defined Fair Use based on other cases that can reasonably be interpreted to mean the following:

- You can rip music that you have legally purchased to MP3s so that you have them in a digital format.
- You can store the songs in your computer or MP3 player, for you own personal use.
- You can burn your own “mix” CDs using your own CD collection, as long as you keep that mixed CD in your possession.
- These same principles apply to movies, books, or any other copyrighted material that you may own.