Acceptable Use of Technology

Acceptable Use of Technology

Overview

To define what users may or may not do in the process of utilizing Cincinnati State IT systems and resources, acceptable use of technology policies are provided.

Scope

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

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

Policy Statement

Cincinnati State provides communications services for the convenience and efficiency of students, employees, and school-approved business partners for use in the course and scope of conducting business for or with the school. All messages and documents sent or received through these communications services and/or stored on Cincinnati State-owned or controlled computers, servers, or other devices are subject to Cincinnati State integrity standards.

Definitions

Students are individuals taking courses, credit or non-credit, degree-seeking, or non-degree-seeking at the College, and those who attend other educational institutions at a Cincinnati State location or who participate in an online relationship with Cincinnati State (in a high school dual enrollment program, for example). Individuals who are not specifically enrolled for a specific term but who have a continuing relationship with the College are considered students.

Employees are individuals classified as full-time, part-time (including adjunct faculty), or temporary employees of Cincinnati State including student workers.

College refers to Cincinnati State and its subsidiaries, divisions, and affiliates.

Business Partners are individuals or firms considered customers and suppliers of the College, including contractors and consultants.

Communication Services, for the purposes of this policy, are messages and documents sent or received via letter, memo, telephone, voicemail, fax, audio/video tape, computer media, file/print servers, electronic mail, online computer services (internet, Google, etc.), instant messaging, wireless message devices or any other means provided by the College or conducted over College resources.

Controls

Content

Communications Services are provided for the convenience and efficiency of users in the course and scope of performing their duties for the College. Although they sometimes may be intended to be confidential, all communications may become subject to discovery in a civil or criminal proceeding, or to disclosure in response to a valid request for documents under the Ohio Public Records Act. The contents of electronic communications (e-mail, fax, computer files, etc.) and voicemail messages may have the same status as paper records.

The following types of messages are strictly prohibited:

- Messages with threatening, harassing, abusive, embarrassing, vulgar, sexual, racially offensive, defamatory, indecent content or implication, or anything else contrary to any Cincinnati State policy.
- Messages proposing any type of commercial transaction, including sales or trades (such as "want ads"), chain letters, betting pools, gambling, political announcements or solicitations, 'junk' e-mail or e-mail posted on a bulk basis to multiple recipients or other solicitations and distributions that are not related to Cincinnati State.
- Messages that violate any law, regulation, or Cincinnati State policy, including, for example, copyright or employment laws.
- Messages that disclose any confidential or proprietary information of Cincinnati State to any employee, business partner, or other third party having no business-related need to know the information.
- Messages or communications disclosing sensitive Cincinnati State data (such as posting messages on internet "chat rooms") unless said messages are authored by a designated Cincinnati State spokesperson.

Communication between employees must be carefully thought out. The ease of use and instantaneous nature of e-mail sometime lulls the user into making statements that he or she would never have made using written memos. Messages and material downloaded from the Internet and sent by e-mail can give rise to legal action against Cincinnati State and its employees. Therefore, no one may put something into an e-mail message that they would not put down on paper, and voice mail may not be appropriate for certain confidential communications. When using e-mail for confidential communication, use caution and make sure that the person to whom you are sending the communication knows that you are sending a confidential message by, for example, putting the word “confidential” in the subject line.

College-wide Message Distribution

In the event an employee (other than system administrators) wishes to use Cincinnati State communications services for distribution of a Cincinnati State-wide message, said message must be approved in advance by the Human Resources Department and/or the Marketing & Communications Department of the highest level that represents the audience to which the information will be sent.

Guidelines for Protection of Confidential Communications

Employees must take appropriate steps to safeguard all sensitive or confidential information regardless of the method of communication. Depending on the circumstances and the nature of the confidential information, appropriate steps may include:

- **Fax**: ensuring that the actual recipient or recipient's designee is present at the receiving fax machine.
- **Email**: sending the message via a file attachment that is password-protected or with encryption enabled. Consult with Information

Technology Services for further details and requirements on encryption and before you encrypt any data.

- **Voicemail**: avoiding communication via voice mail. Direct telephone contact with the recipient may be necessary. Using speakerphone in public areas, pay phones in high traffic areas such as airports, and analog mobile (vs. digital encrypted) telephone services are usually not appropriate when sensitive or confidential information is to be discussed.
- **Interoffice Mail**: having sensitive or confidential information hand delivered whenever possible. When this is not possible, notify the intended recipient via telephone to expect the mailing and send the information in a solid, sealed container (envelope, box, etc.) labeled “confidential”.
- **Public Mail**: sending with registration, return receipt requested, and/or other means to verify that the intended recipient received it. Notify the intended recipient via telephone to expect the mailing.
- **Print**: avoiding the use of printers located in open, generally available areas (e.g., departmental network-based printers) when printing sensitive or confidential information unless the person printing the information is present at the printer to ensure privacy.
- **Internet Services**: sensitive or confidential information must not be disclosed via an internet or other online service bulletin board, social media platform, chat room, usenet news bulletin, or any other messaging service.

Where e-mail messages do contain confidential information, they must be clearly marked “confidential.” They must also incorporate a warning if they reach anyone other than the intended recipient, which must read as follows:

"This transmission is intended only for use by the intended recipient(s). If you are not an intended recipient you must not read, disclose, copy, circulate or in any other way use the information contained in this transmission. The information contained in this transmission may be confidential and/or privileged. If you have received this transmission in error, please notify the sender immediately and delete this transmission, including any attachments."

If you intend to rely on the contents of an e-mail at any future date, a separate hardcopy must be kept on file. The e-mail must not be stored electronically.

Personal Use of Communication Services

Occasional personal use of Cincinnati State communications services can Cincinnati State students and employees. The following rules apply to such usage:

- Students should use their Cincinnati State e-mail accounts primarily for communications related to their educational endeavors.
- Personal use of Cincinnati State communications services must in no way impact the employee's ability to perform job functions at acceptable levels.
- Personal use of Cincinnati State communications services may in no way conflict with other policies, procedures, or guidelines.
- Personal use of Cincinnati State communications services must be confined to the employee's own time (e.g., before/after business hours, during lunch, during breaks as defined by Human Resources policy). Personal use for commercial purposes not related to Cincinnati State business is prohibited.
- Under no circumstances are personal documents, messages, social media posts, chat room conversations, usenet news bulletins, pictures, or other communications to be posted to an internet or other online service from a Cincinnati State e-mail address, user ID, or server.

Monitoring & Disclosure

It is critical that Cincinnati State be able, for its legitimate business purposes, to access and monitor all Cincinnati State communications services. Legitimate business purpose include (without limitation) such activities as: (a) legal or contractual obligations to produce any communication or audit any communication process; (b) retrieval of data from back-up or archive for system functioning; (c) network and system security; (d) safeguarding of Cincinnati State confidential information; (e) prevention of publicity adverse to Cincinnati State; (f) prevention of sexual harassment and workplace intimidation; (g) enforcement of Cincinnati State policies (particularly those on authorized use of IT); and (h) management and control of costs and capacity of Cincinnati State IT systems.

Any automated monitoring that might be used by Cincinnati State would be applied to all communications in a particular communication channel and would not be directed at any specific employee. That said, the College may request, through Human Resources and/or Public Safety, monitoring a specific employee for a specific reason. Generally, it is not practical for Cincinnati State to have separate access control and monitoring systems for business and personal use. Accordingly, all users of Cincinnati State communications services must expect that the following can be accessed or monitored for legitimate business purposes.

- Messages sent or received via Cincinnati State-provided internal or external electronic communications services, including e-mail and voice mail
- Data or software stored on Cincinnati State-owned computers, servers, storage media or other devices
- Usage of the internet or Cincinnati State intranets

No facilities are provided or maintained for private or confidential e-mail, voice mail or computer files. Cincinnati State may:

- Authorize security personnel system administrators, and/or supervisors to review and/or monitor electronic or voice mail messages and/or data or software contained on Cincinnati State computers, servers, storage media or other devices on a periodic, random and/or ongoing basis to ensure compliance with this policy, for other purposes authorized by law or as part of an investigation
- Grant access for other staff, for necessary business purposes, to access data or software stored on Cincinnati State equipment

Violations

Any student or employee found to have violated Cincinnati State policy related to access or use of Cincinnati State communications services will be subject to disciplinary action up to and including termination (employees) or expulsion (students).

In addition, subject to local, state, or federal laws, employees could face criminal charges resulting in a fine or imprisonment.

Internet Usage

Cincinnati State provides access to public information networks for the convenience and efficiency of students and employees in the

course and scope of conducting business for Cincinnati State. It is the responsibility of each user to closely adhere to the following with respect to his or her use of all public information networks (e.g., the Internet).

Introduction

Cincinnati State provides access to public information networks, such as the Internet, as an information and communications tool. While Cincinnati State recognizes that use of these public networks offers tremendous benefits, these public networks can create exposure to potentially damaging risks, including liability due to careless communication, exposure to computer hackers and viruses, and potential loss of productivity. When using the Internet in the context of their job (employees) or because of academic necessity (students), users shall be cognizant of the implication of their communications. They shall consider that their communications can create the same impression as a memo printed on Cincinnati State letterhead. Hence, each user has a responsibility to ensure that when using the Internet on the job (employees) or because of academic necessity (students) that any communications are in accordance with the nature and context of the user's job responsibilities (employees) or because of academic necessity (students).

Usage

Access to Cincinnati State's resources is a privilege, which is allowed only to the College's authorized personnel and students. All users must understand and abide by the responsibilities that come with the privilege of use. Such responsibilities include, but are not limited to, the following.

- You must understand and comply with all applicable federal, state, and local laws.
- You must not intentionally seek information about, browse, copy, or modify non-public files belonging to other people. You must not attempt to "sniff" or eavesdrop on data on the network that is not intended for you.
- You are authorized to use only computer resources and information to which you have legitimately been granted access. Sharing your password with others is expressly forbidden. Any attempt to gain unauthorized access to any computer system, resource or information is expressly forbidden. If you encounter or observe a gap in system or network security, immediately report the gap to the ITS department.
- The College's policy on harassment applies equally to electronic displays and communications as to the more traditional (example, oral or written) means of display and communication.
- Messages, sentiments, and declarations sent as electronic mail or postings must meet the same standards for distribution or display as physical (paper) documents would on college property.
- Unsolicited mailings and unauthorized mass mailings from campus networks or computing resources (SPAM) are prohibited.
- Spoofing, or attempts to spoof or falsify email, network or other information used to identify the source, destination or other information about a communication, data or information is prohibited.
- You must not degrade computing or network performance in any way that could prevent others from meeting their educational or College business goals. You must not prevent others from using shared resources by running unattended processes, by playing games or by "locking" systems without permission from the appropriate system manager.
- You must conform to laws and College policies regarding protection of intellectual property, including laws and policies regarding copyright, patents, and trademarks. When the content and distribution of an electronic communication would exceed fair use as defined by the federal Copyright Act of 1976, users of campus computing or networking resources must secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations, and computer software.
- You must not use college computing or networking resources, or personal computing resources accessed through college network facilities to collect, store, or distribute information or materials, or to participate in activities that are in violation of federal, state, or local laws.
- You must not use college computing or networking resources, or personal computing resources accessed through college network facilities to collect, store, or distribute information or materials in violation of other College's policies or guidelines. These include, but are not limited to, policies and guidelines regarding intellectual property and sexual or other forms of harassment.
- You must not create or willfully disseminate computer viruses, worms, or other software intended to degrade system or network security. You must take reasonable steps to prevent your system from being used as a vehicle for such actions. This includes installing system and software patches as well as anti-virus signatures files.
- Use of Cincinnati State's resources for advertising, selling, and soliciting for commercial purposes or for personal gain is prohibited without the prior written consent of the College.
- The disclosure of individually identifiable non-directory information to non-university personnel is protected by the Family Educational Rights and Privacy Act of 1974 (FERPA). The disclosure of financial or personnel records that are owned by the College without permission or to unauthorized persons is not permitted and may be prosecuted under Ohio Law.
- Willful or unauthorized misuse or disclosure of information owned by the College will also constitute just cause for disciplinary action, including dismissal from school and/or termination of employment regardless of whether criminal or civil penalties are imposed. It is also expected that any user will report suspected abuses of college resources. Failure to do so may subject the individual to loss of network access and/or the disciplinary action referred to above.

The college's ITS department may immediately suspend service to an individual or computer found to be significantly degrading the usability of the network or other computer systems. Inappropriate use will be referred to the appropriate College authority to act, which may result in dismissal from school and/or termination of employment.

Insider Information

It is the policy of Cincinnati State to comply with all relevant state and federal civil and criminal securities laws which, among other things, prohibit insider trading. An employee may be held liable for violating state and federal civil and criminal laws if they trade in securities while in possession of material, non-public information regarding the business of the College or disclose or tip material, non-public information to another person who subsequently uses that information to his or her profit. These laws are severe. It is imperative that each user of any public information network exercise extreme caution when

disclosing information about the college. Dissemination of non-public information over the Internet is strictly prohibited by the college and is grounds for immediate dismissal.

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

Additional information about technology-related policies and procedures is available in the Information Technology Services section of the College intranet. Students and employees must login to MyCState 2.0 to access this information.

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/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.