Information Technology Policies
Publication 12.0.PUB1 (February 2026)

CCMS provides computing and network resources to its students primarily for educational purposes. CCMS may provide access to other users at its discretion. Use of CCMS's computing and network resources is a privilege, which can be revoked at any time. All users are expected to exercise personal and professional responsibility and integrity when using these resources. Each user must understand and acknowledge that his/her freedom to access and display information is constrained by the rights of others.

POLICY VIOLATIONS

If a student violates any of the acceptable use provisions outlined in this document, his/her computer privileges will be terminated, and future access may be denied. Some violations constitute a criminal offense and may result in legal action and/or other penalties as deemed warranted by the President of CCMS.

Copyright Policy

Copyright Law (Title 17, U.S. Code) provides legal protection of intellectual property in whatever medium. Protected works include, but are not limited to, literary, dramatic, musical, artistic, pictorial, graphic, film and multi-media works. These include books, magazine articles, software, digital works, motion pictures, sound recordings, and unpublished works, among others. A copyright owner has the exclusive right to reproduce the work, prepare derivative works of the work, distribute copies or recordings of the work, perform the work publicly, including by means of a digital audio or video transmission, and display the work publicly.

- Violations of Copyright laws can result in civil penalties, including actual or statutory damages, as well as criminal prosecution.
- CCMS is committed to remove, take down or otherwise block access to infringing material whenever it is brought to our attention and whether or not the individual who is infringing has received notice.
- Important to an educational institution, under the Copyright Act, is the "fair use" doctrine, which excludes from the limits of copyright law the use of intellectual property for purposes such as criticism, commentary, news reporting, teaching, scholarship or research. This allows educators and students to use copyrighted materials, in certain circumstances, without having to get permission from the author or copyright owner. "Fair use" is not absolute but rather must conform to the guidelines of the U.S. Copyright Office on what constitutes fair and acceptable use in an educational setting.
- Please report all violations or concerns about Copyright Law to the Director of Library & Information Technology, who will investigate and take all appropriate measures to remedy the situation. CCMS monitors its network, maintains firewalls to deny access to certain websites known for unauthorized copyrighted materials, and may deny access to

any student violating this policy, as well as apply any other sanctions available to it. CCMS, no less than annually, using relevant assessment criteria, shall review the effectiveness of its program to combat the unauthorized distribution of copyrighted material.
- CCMS, through its Director of Library & Information Technology, may provide legal alternatives for accessing and downloading copyrighted material.

Email and Accountability

A CCMS-provided email address (username@students.ccms.edu) is an official means of communication. Students are responsible for all CCMS communication sent to their CCMS email address. Students must check their email account on a frequent and consistent basis. CCMS communicates regularly to students via email, thus it strongly suggested that students check their email at least once every day. CCMS advises students to respond to all official CCMS communications as directed in each communication (e.g., responding in person, in writing, or by email). Students should not assume an email response is a satisfactory substitution when directed otherwise. This email policy applies from orientation and continues through the academic terms for which they are enrolled, including during breaks, holidays, vacations, and periods of suspension.

- Students may forward their CCMS email to another email address. However, CCMS is not liable for any problems that may result from forwarding CCMS messages to another email account (e.g., problems with spam filters, full mailboxes, or loss of attachments). Forwarding CCMS email may have the unintended consequence of exposing privacy information to third parties because Internet-based email is handled in a public fashion.
- Students should not use their CCMS email for bulk emails, forwards, chain mails unrelated to the essential functions CCMS. Students should not open attachments from unknown sources.
- CCMS employs various measures to protect the security of its computing resources and users' accounts. However, CCMS does not and cannot guarantee such security. Furthermore, individuals must exercise caution when sending sensitive or FERPA-protected student information via email. In addition, some College information is not appropriate for email communication.
- CCMS hereby advises its students that all electronic data may be reviewed and/or accessed in accordance with CCMS's policies. CCMS has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.
- After graduation, CCMS permits the graduating student to retain his/her email address for an additional 18 months subject to the provisions of this policy. This is a privilege, which may be revoked at any time for any reason. After the 18 months or if revoked earlier, CCMS will terminate the account and all contents therein. CCMS will terminate the accounts of student users who do not graduate when that student is no longer active. CCMS in no way warrants the contents of any email account, and has no duty of preservation.

Student Information Security

Cyber and physical threats put CCMS and its students at risk. The Gramm-Leach-Bliley Act requires CCMS to develop and maintain an information security program to minimize risk to students and safeguard sensitive data. CCMS has designated its IT services provider as the Qualified Individual responsible for overseeing, implementing, and enforcing the College's

information security program. The Dean of the College serves as the senior member of the College's personnel responsible for direction and oversight of the Qualified Individual.

The College's IT services provider regularly conducts a risk assessment that defines reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student information that could result in unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks. Criteria for assessing security risks include vulnerabilities determined from scans of both the external environment and the internal environment.

When a risk is identified, the risk is addressed by technological scans for vulnerabilities. Vulnerabilities are categorized into four areas: Critical; High; Medium; Low. Vulnerabilities from known exploits are determined as critical or high. Critical or High vulnerabilities are labeled priority 1 and must be addressed prior to the next scheduled scan. Medium vulnerabilities are labeled priority 2; low vulnerabilities are labeled priority 3.

Risk assessments are periodically performed at least quarterly and include reviewing access controls. Multifactor authentication is used for any individual accessing any of the College's information systems. The IT services provider uses qualified information security personnel to manage information security risks and to perform and oversee the information security program. The College's contract with the IT services provider requires the provider to implement and maintain appropriate security safeguards. When a risk incident is identified, the College, along with the IT services provider, evaluates and adjusts the information security program to mitigate any potential repeat occurrence of the risk and make corrective action.

CCMS requires that all passwords are "strong." Students must immediately report to the Director of Learning Resources and Student Services the discovery of any malware, such as viruses, spyware, and botnets, on any CCMS computer. CCMS further advises that devises from which students access their CCMS email account should meet the minimum security requirements set forth in this policy, including anti-malware protections; secure connections, updated operating systems and software, and encryption.

Populi Privacy Policy

In addition to the privacy policies set forth in the Student Handbook, Populi, CCMS's online student information system provided by the third-party (Populi) protects the information collected from or about students and CCMS, including private personally identifiable information, from unauthorized access, use, or disclosure. Because transmitting information over the Internet or storing information is not always completely secure, Populi cannot guarantee the absolute security of any information, but it does take reasonably necessary measures to do so.

Prohibited Actions

No student, employee or agent of the Cincinnati College of Mortuary Science will utilize CCMS' information technology, including but not limited to, computers, network, email account, fax machine, copy machine, or telephones, for the following:

- preparation and/or transmission of any illegal or unlawful communication including, but not limited to, obscene or sexually explicit material, libelous or slanderous communications, or communications intended sexually or otherwise to harass or improperly discriminate on the basis of sex, gender identity, race, color, economic status, class, religion, culture, national origin, citizenship, veteran status, ethnicity, sexual orientation, position, age, handicap, or disability;
- any action that violates system security;
- in violation of copyright law;
- use of the Internet in general, and social media sites in particular, as a venue and/or platform for discussing any aspect of the care and/or treatment of deceased human beings, including, but not limited to, embalming and restorative art classes, human anatomy lab class, clinical rotations and any other course in which the topic of discussion is of a sensitive and confidential nature; and
- changing, modifying, or eliminating library computer configurations and loading any application or program software onto the library computers.

This list is not all inclusive.