

COPPER MOUNTAIN COLLEGE
COMPUTER USE PROCEDURES/ELECTRONIC MEDIA USE GUIDELINES
For Students

PHILOSOPHY

- Student access to electronic information systems at Copper Mountain College District (CMCCD) is a privilege and must be treated as such by all student users.
- This access may be limited or revoked if CMCCD policies are not followed.
- All users are expected to abide by these policies when accessing the Internet through the network connection.
- Acceptance of any access account and/or use of the CMCCD electronic network constitute an agreement to abide and be bound by the provisions of the applicable procedures and policies regarding its use.
- Ignorance of the applicable CMCCD policy and procedures is not a defense in issues regarding access to electronic information systems at CMCCD.

STUDENT LOGIN:

- Registered students will be assigned a personal account on the CMCCD student information system (SIS) known as *Coyote Tracks*.
- Students who log in to *Coyote Tracks* will have access to a variety of information through the Datatel portal.
- Students often use external email accounts, such as Hotmail or other public email system providers for approved educational activity – this is generally acceptable, assuming compliance with all other aspects of this policy.
- When a student suspects that their password has been compromised, it is their responsibility to report this information to their instructor or the Information Services Department as soon as it is discovered.

DISK STORAGE SPACE

- Space for storing data on networked computer systems is a limited resource therefore student users should not save unnecessary files and should delete files that are no longer needed.
- Information and files stored by students are generally purged after each full semester.
- In limited circumstances and with sufficient notice, I.S. staff may act on requests to have information carried over from one semester to the next for students enrolled in the next semester, or to assist students in copying their information to appropriate student supplied media before purging.

USE OF EXTERNAL NETWORKS

- Most systems connected to the CMCCD SIS_network have access to the Internet. However this may not be true of *all* systems.

NETWORK INTEGRITY

COPPER MOUNTAIN COLLEGE
COMPUTER USE PROCEDURES/ELECTRONIC MEDIA USE GUIDELINES
For Students

- Tampering with any network cabling or routing devices is expressly prohibited.
- Any problems with these devices or cabling will be serviced by I.S. Department.
- No one may extend the network to another room or building, except the I.S. Department.

COMPUTER SOFTWARE NOT OWNED OR LICENSED TO CMCCD

- Student installation of *any software* program is prohibited.
- Exceptions may be granted, on an individual basis by the I.S. Department, as needed in the daily conduct of the course in which the student is enrolled.
- This software must conform to the purpose of the course, student learning outcomes, or assist with student success in the course. Examples include:
 1. office templates
 2. stationary
 3. audio utilities
 4. video utilities (ex: Real Player)
 5. digital images
- Any such software must be pre-approved by the instructor, or the I.S. Department.

STUDENT CREATED PROGRAMS AND WEB SITES

- Students may have occasion, during the course of their education, to create software programs and originate individual web sites using CMC computer resources.
- These must comply with all College policies as well as Federal, State, and Local laws and regulations.
- In addition, they must not violate copyright laws, and obscenity laws.
- Further, they must conform with laws relating to libel, slander, defamation, and software piracy.

USE OF ELECTRONIC RESOURCES

- Copper Mountain College computing resources and network are for the use of CMC faculty, registered students, staff and general public.
- These resources are to be used only for the academic, administrative, educational, and research purposes of the institution and workforce preparation.
- Copper Mountain College acknowledges that registered students may, on occasion, use CMC computing resources to which they are granted access for non-commercial, personal use (for example, email).
- Such occasional non-commercial use is permitted if the use is not excessive and:
 1. does not interfere with the performance of any faculty, staff member, or student's duties
 2. does not interfere with the efficient operation of the network or its computing resources

COPPER MOUNTAIN COLLEGE
COMPUTER USE PROCEDURES/ELECTRONIC MEDIA USE GUIDELINES
For Students

3. Is not otherwise prohibited by local, regional, State, Federal laws or directives, or any other CMC policy, procedure, or directive.

PRIVACY OF ELECTRONIC FILES

- Information and messages stored on or sent over the CMCCD network, however, are not secure and can be intercepted in a variety of ways.
- CMC students accessing the network cannot assume such information will be or remain inaccessible or confidential.
- Each student user is expected to maintain the confidentiality of all information stored on computing resources to which he or she has access.
- However, the system administrator may access user files as required to protect the integrity of computer systems. For example, following organizational guidelines, the system administrator may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have become corrupt or damaged.
- *Requests for the disclosure of confidential information is governed by the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA) and other applicable Federal, State, and Local Law.*

NON GUARANTEE OF PRIVACY

- CMCCD cannot and expressly does not guarantee student user privacy.
- CMCCD reserves the right to inspect and examine any District owned or operated computer system, computing resource, and/or file(s) or information contained therein at any time in response to security threats to the system network or CMCCD members, to investigate claims of violations of this policy or other policies, and when system/network maintenance identifies possible security threats or violations.
- If the Information Services (I.S.) Department gains evidence that stored student files contain inappropriate content those files are subject to review without notice by the appropriate staff.

PROHIBITED USE OF ELECTRONIC RESOURCES

- Personal use of computing resources by any student user for personal financial gain in connection with non-CMC consulting, business, or employment is strictly prohibited.
- Any student use of CMC computing resources in conjunction with non-CMC professional consulting, business, or employment activities is permitted only when the use has been expressly authorized in writing by the administration at the appropriate level.

EXAMPLES OF PROHIBITED ACTIVITIES:

Examples of activities that would violate one or more of the guidelines, meant to be *illustrative*, not exhaustive, include:

COPPER MOUNTAIN COLLEGE
COMPUTER USE PROCEDURES/ELECTRONIC MEDIA USE GUIDELINES
For Students

- a. Advertising of commercial products, services and businesses that are not affiliated with or sanctioned by CMC.
- b. Using CMCCD printing facilities to produce output that is not related to the College's mission (i.e., it is not acceptable to print announcements or fliers for outside agencies, materials for a student's own or a spouse's business, etc.).
- c. Disrupting a CMCCD employees work in any way, such as tampering with network electronics or interfering with an active client computer or network server.
- d. Sending messages that cause an ongoing interruption in the work of another person such as sending email after the recipient has requested that it be stopped, sending email indiscriminately to large groups of users, playing music through speakers, or transferring large amounts of data that might cause congestion of the network. etc).
- e. Printing large documents or photos not directly related to course work.
- f. Sending chain letters and broadcast messages to *lists* or individuals,
- g. Altering, disabling, or removing any software which resides on a machine in CMC's public computing areas or accessible via our network.
- h. Connecting *any* personal electronic device to the campus administrative network, **specifically a lap top or desk top computer. Data transfer by a USB stick or digital camera is an acceptable activity on the student network for academic use. Where available, WIFI permits public access to the student network.**
- i. Sharing a CMCCD password to an account with anyone, including another student, an employee, spouse, parent, dependent, or friend.
- j. Physically tampering with, disabling, or removing any equipment, wiring, or networking hardware from the public computing areas, classrooms, offices, or equipment areas.
- k. Possessing or using any software or hardware designed to disrupt the security of the campus network or any devices attached to the network.
- l. Engaging in any activities designed to spy on the network traffic of other users.
- m. Viewing, storing, or electronically downloading pornographic material of any type.

EMAIL, EMAIL HARASSMENT AND RELATED ISSUES

- Harassment and any other form of intimidation via the network are strictly prohibited.
- This type of inappropriate behavior is not acceptable on the network, and all incidents will be dealt with according to established policy and law.

ACCEPTANCE OF THE CMCCD ELECTRONIC MEDIA USE GUIDELINES

- These guidelines reflect the general ethical principles of the college community and indicate the responsibilities that are characteristic of the college's computing environment as it applies to all students.
- Registration and matriculation automatically affirm their agreement to comply with these principles, procedures and guidelines.