COLORADO MESA UNIVERSITY	**Computer Use Policy**	
	Revised: January 15, 2021	**Page: 1 of 4**

I. Purpose

Colorado Mesa University provides students, faculty, and staff the privilege to use its computers and network for the purposes of accessing software, information systems, and the Internet in support of the institution's mission.

The purpose of the Computer Use Policy is to ensure users of the University's computing systems and networks are aware of their rights and responsibilities with respect to appropriate use of computers and networks, including the storage of confidential information; security practices; and software compliance and copyright law.

II. Definitions

"Confidential" means a restriction placed on access to information by federal or state laws (including administrative regulations), court orders and rules, contracts, licenses, or Trustee and University policies.

"Computer" means any university-owned desktop or mobile computing device used for instruction , research or administrative purposes.

"Employees" means all full and part-time, temporary and regular University employees including faculty members, administrators, classified personnel, and student employees.

"Mobile Computing Devices" means laptops, tablets or smartphones, etc.

"Monitor" means to intercept, access, or inspect an electronic communication. "Monitor" does not include automatic scanning of an electronic communication by network security software such as firewall and anti-virus programs.

"Network" means the University local area network, wireless network, or wide area network.

"Students" means students who are currently enrolled and in good standing at the University.

"User" means a student, employee, or member of the public that uses a University-owned computer, data storage facility, or network.

III. Policy

A. User Responsibilities

Users are responsible for activities originating from their computers or network connection.

Computer Users shall:

- Adhere to University policies and local, state and federal laws, including copyright law, and not use campus resources for any illegal activity or any prohibited uses outlined in this policy.
- Protect their CMU computer login username and password to protect University computers, network and information. This includes not sharing your passwords with anyone or for any reason.
- Follow information security best practices and support strong passwords, never leaving your computer logged on and unattended and never storing confidential information on mobile computing devices.
- Not impede the academic pursuits of other users.

The University is responsible for the reliability and security of its computer systems and network. Colorado Mesa University's Department of Information Technology reserves the right to suspend user accounts or disconnect any computer or network-attached device, without warning, which poses a security or performance risk to the campus systems and network. Inappropriate user computer activity may result in the loss of computer privileges.

B. Software Compliance

Users shall use software in accordance with terms of license agreements and copyright laws. CMU does not have the right to reproduce software or related documentation without proper written authorization. The unauthorized copying or redistribution of copyrighted software is illegal. CMU reserves the right to impose disciplinary and/or legal action as deemed appropriate.

C. Permissible Use

University computers and networks are provided for the academic and administrative objectives of the University and shall be used in a manner consistent with the purpose for which they are provided. University-owned computers in academic areas shall not be used for recreational use, games or display of images that may create a visibly hostile environment.

D. Prohibited Use includes, but is not limited to:

a) Sending or storing confidential information without authorization;
b) Using University computers, networks, or resources for unauthorized commercial purposes;
c) Using a computer account that you are not authorized to use;
d) Illegally downloading and distributing copyrighted material, such as software, movies, music, and games, through the use of peer-to-peer (P2P) networking;
e) Violating terms of software agreements or copyright laws;
f) Using the University computers or networks to gain unauthorized access to any computer system;

g) Utilize any personal computing device to gain unauthorized access to network resources;
h) Bypassing, disrupting, or disabling security controls or operation of the campus network or computer systems;
i) Knowingly installing or spreading malicious software such as viruses and worms, or otherwise attempting to disrupt the performance of another computer system or network;
j) Congesting the campus network and Internet bandwidth and hampering the productivity of other network users;
k) Participating in any illegal activity including, but not limited promoting child pornography, distributing obscene material, threatening the safety of persons, etc.;
l) Using University computers or networks to harass an individual or group or for any other action against University policy; and
m) Monitoring, deleting, or tampering with another user's electronic communication or files without proper authorization.
n) Installation of software on university owned equipment without the prior approval of the IT department.

IV. Enforcement

A. Violations

Computer Use Policy violations may result in the suspension of the user's computer account without warning, and users involved in a major infraction may lose their computer and network privileges indefinitely. Suspected violations of the Computer Use Policy will be handled by the Director of Computing and Network Systems.

Student violations of the Computer Use Policy are considered an infraction of the Student Code of Conduct. Student users found to be responsible for an infraction will be referred to the Student Conduct Officer and are subject to sanctions in accordance with the Student and Academic Policies Guide. The student appeal process is outlined in the Student Code of Conduct.

Employee violations of the Computer Use Policy are considered unprofessional conduct. Employees may be subject to disciplinary action in accordance with the *Colorado Mesa University Trustees Policy Manual*, the *CMU Professional Personnel Employee Handbook*, and/or the *State Personnel System Employee Handbook* as applicable.

Users of University computers and network are responsible for respecting and adhering to local, state and federal laws. Any attempt to break those laws through the use of University resources may result in civil or criminal action against the offender by the proper authorities. If such an event should occur, Colorado Mesa University will fully comply with the authorities and legal requests for information.

B. Monitoring

The University may monitor, without warning or notification, computer and network activity under the following circumstances: 1 required to maintain or protect campus computers, networks or property; 2

based on an individual suspicion or report that a student or employee has violated this Policy or other University policy, or local, state or federal law; or 3 limited in scope to an investigation of the suspected violation as part of a warrant, subpoena, or court order.

C. Reporting Policy Violations

Report cases of inappropriate computer or network uses of University computers and network to the Information Technology department at ITsecurity@coloradomesa.edu.

V. Related Policies

Electronic Communications Policy

Student and Academic Policies Guide

Policy and Plan to Combat Unauthorized Distribution of Copyrighted Material and Peer-to-Peer File Sharing