I. Purpose

Colorado Mesa University ("University") provides its employees and students the privilege to use University-owned or operated electronic communication facilities for the academic and administrative objectives of the University.

The purpose of the Electronic Communications Policy is to ensure users of the University's electronic communication facilities are aware of their rights and responsibilities with respect to appropriate use; e-mail privacy; monitoring and disclosure of electronic communication; and storing, retaining and archiving electronic communication.

This Policy supplements and does not supersede other University policies governing the appropriate or acceptable use of computing and network facilities.

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.

"Content" means any information concerning the substance, purport, or meaning of an electronic communication.

"Data Protection Plan" refers to the University's Data Protection Plan for established data governance structure, which defines roles and responsibilities for data stewardship; defines classifications for University data based on levels of sensitivity; and outlining guiding principles for properly protecting University data.

"Direct cost" means a cost, fee or charge that would not otherwise be incurred by the University (e.g. printing costs and lost work time).

"Electronic communication" includes any electronic communication that has been sent, published, or received by employees or students using University-owned or operated electronic communication facilities or personal devices for university-related activities. Electronic Communication incudes, but is

not limited to, electronic mail (email), instant message, text, social media, collaborative workspaces (e.g. SharePoint), and facsimile (fax) communications.

"Electronic communication facilities" includes, but is not limited to public, private, and commercial computer networks (including the Internet), and facsimile equipment.

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

"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.

"Students" refers to students who are admitted or currently enrolled at Colorado Mesa University

“Public Record” includes all writings maintained or kept by the University for the use in the performance of public functions or involved in the receipt of public funds.

“Transitory Communication” is casual or routine electronic communication with no real value to the University.

III.Policy

A. Permissible Uses of Electronic Communication Facilities

Except as expressly permitted below, University-owned or operated electronic communication facilities are intended and shall be used solely 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.

The University acknowledges that employees occasionally use e-mail and the Internet for personal purposes. However, personal use is prohibited if it entails a direct cost to the University or interferes with the employee’s performance of job duties.

The University reserves the right to place additional restrictions on student and employee personal use of its electronic communication facilities if necessary or convenient to conserve network resources for academic and administrative objectives.

B. Prohibited Uses of Electronic Communication Facilities

The following uses of the University’s electronic communication facilities are prohibited:

1. Unauthorized commercial purposes;
2. Breach or attempt to breach the security of any electronic communications facility (including the unauthorized or intentionally deceptive use of network privileges, accounts, access codes, identifiers or passwords); access or use of any electronic communication facility without authorization; or knowingly intercept, access, disclose, alter, disrupt, damage, or destroy any electronic communication, or any data, software, or hardware without authorization;
3. To intentionally disrupt or interfere with another user of any electronic communication facility;
4. Send, store or utilize confidential information without authorization;
5. Infringe copyrights or violate other intellectual property rights and laws;
6. Threaten, intimidate, harass, or defame others;
7. Violate any other University policies or local, state and federal laws.

C. E-mail Privacy

Current e-mail technology does not guarantee privacy. Information about e-mail, including the sender's and recipient's names and addresses, the date and time, and the content of the communication, is automatically recorded by the computer networks over which it is transmitted and may be backed up and stored for periods of time. Others in addition to the sender and recipient may have authorized or unauthorized access to some or all of this information. Unauthorized access to or disclosure of an email may occur in the event of a compromised computer account; by human error of sender typing the wrong e-mail address or the recipient forwarding a communication to a third-party; or loss of a mobile device where the user's e-mail is synchronized and not password protected.

Because privacy cannot be guaranteed, it is important to exercise good judgment in drafting and sending e-mail. Do not use e-mail to communicate confidential information; information that would be embarrassing or damaging to you or others if it were received by the wrong person or made public; or in an unprofessional manner.

D. Text Messaging

The University shall only use text messaging to enhance communication with students and employees for emergency warnings/safety notifications and authorized student success initiatives. This Policy does not include text messages sent to prospective students. Text messages sent for the purposes of student success shall be professional, individually targeted messages that communicate such items as upcoming deadlines and appointment reminders. Text messages may not include private information protected under the Data Protection Plan and shall not release any identifiable information protected under FERPA. System generated group text messages shall 1) include an option for the recipient to opt-in/opt-out of receiving text messages, 2) be accessible for all intended recipients, and 3) be professional and not include text abbreviations.

E. Monitoring and Disclosing the Content of Electronic Communications

1. General

The University does not routinely monitor or disclose the content of electronic communications sent, received, or stored using University-owned or operated electronic communication facilities.

2. Exceptions

As the owner or operator of electronic communication facilities and a public institution of higher education subject to the Colorado Open Records Act, § 24-72-200.1 et seq., C.R.S., as now and hereafter amended, the University may monitor or disclose the content of electronic communications under the following circumstances:

a. A party to the communication consents;

b. The communication is readily accessible to the public (e.g., a public Web page, e-mail sent to a public mailing list, or social media post);

c. Monitoring or disclosure of an electronic communication is in the normal course of University employees' employment and is necessarily incident to the maintenance of the University's electronic communication facilities, the rendition of electronic communication services, or the protection of the University's rights or property (examples include but are not limited to routine maintenance, troubleshooting, or investigating an excessive use of network resources that adversely affects performance);

d. Monitoring or disclosure of an electronic communication is: (i) based on an individualized suspicion that an employee or student has violated this Policy, other University or Trustee policies, or state or federal law; and (ii) limited in scope to an investigation of the suspected violation; or

e. The University is legally obligated to monitor or disclose an electronic communication by warrants, subpoenas, court orders and discovery requests submitted under the Federal or Colorado Rules of Civil Procedure.

F. Storage, Retention and Archival of Electronic Communications

1. General

State laws and University record-keeping policies apply to records created or stored in digital format including electronic communications. The University does not maintain centralized archives of electronic communications sent or received over its electronic communication facilities. It is the employee's responsibility to archive electronic communications and files sent or received via the University's electronic communications facilities that are covered under State law and University policies.

Individual employees are responsible for storing and archiving copies of electronic communications sent or received by them for at least 90 days unless so directed or if the communications appear to be:

a. E-mail or other electronic documents ordered collected pursuant to a litigation hold; or

b. Records required to be archived under State Archives and Public Records, 24-80-101 et seq., C.R.S., or University record-keeping policies.

Electronic Communications in email form shall be archived by assigning one of the following retention policy tags: 1 year delete, 3 year delete, 5 year delete, 7 year delete and Never delete. Email and any associated attachments not archived will be deleted and purged and will no longer be recoverable after the set retention period.

2. Storing Electronic Communication on Mobile Devices

Electronic Communication stored on mobile devices shall be properly protected by reasonable and appropriate safeguards in order to protect University information. Mobile devices are often at a higher risk of data loss or theft. Therefore, industry standard protection, based on the protection capabilities of the device, will be implemented on all mobile devices containing university data, including electronic communications. University data may only be stored on authorized devices and storage configurations authorized by the Information Technology department.

3. E-mail is the official form of Electronic Communication for Archiving

University employees shall use e-mail for its official means of electronic communication for all instances where electronic communication must be archived as part of an official institutional record or process or decision-making record. Other types of electronic communications may be used for transitory communication that have no institutional value and not required to be archived. However, transitory electronic communication may be required to be disclosed under Colorado Open Records Act.

IV. Enforcement

A. Violations

Electronic Communications 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 Electronic Communications Policy will be handled by the Director of Computing and Network Systems. Further, the University reserves the right to delete any electronic communication that violates this Policy from its electronic communication facilities.

Student violations of the Electronic Communications 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 Electronic Communications 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's electronic communications facilities 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. Reporting Policy Violations

Report cases of inappropriate uses of the University's electronic communication facilities, or threatening, intimidating harassing e-mail to the Director of Computing and Network Systems, Information Technology, or forward the e-mail with your concerns to ITsecurity@coloradomesa.edu.

V. Related Policies

Computer Use Policy

Student and Academic Policies Guide

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