10.13 ELECTRONIC MAIL POLICY

I. STATEMENT OF AUTHORITY AND PURPOSE

This policy is promulgated by the Board of Trustees pursuant to the authority conferred upon it by §23-41-104(1), C.R.S. (1997) and in accordance with the requirements of §24-72-204.5, C.R.S. (1997) in order to establish guidelines for the responsible and efficient use of CSM electronic mail, hereinafter "E-mail," services and to clearly set forth the rights and responsibilities of CSM employees regarding their use of E-mail. This policy shall supersede any previously promulgated CSM policy that is in conflict herewith.

II. POLICY

A. Introduction

CSM provides E-mail services to support the academic, research, and administrative functions of the institution. Employees must be mindful that use of E-mail is a privilege, not a right, and it should be treated as such by all users. Employees are permitted to use E-mail in a prudent manner for personal communications as long as such personal use does not interfere with the employee's performance of his or her job responsibilities or the business use of E-mail by other employees. Since confidentiality is not readily attainable when using E-mail and because many E-mail communications are public records, employees should never use E-mail to send any message that would be a source of embarrassment to the sender, to the recipient, or to CSM if the message were to be seen by others.

B. Definitions

1. E-Mail

An electronic message transmitted between two or more computers or electronic terminals, whether or not the message is converted to hard copy format after receipt and whether or not the message is viewed upon transmission or stored for later retrieval. E-mail includes electronic messages that are transmitted through a local, regional, or global computer network.

2. Public Records

All writings made, maintained, or kept by the State, or any agency, institution, or subdivision thereof, for use in the exercise of functions required or authorized by law or administrative rule, or involving the receipt or expenditure of public funds.

C. Scope of Policy

All E-mail communications and associated attachments transmitted or received over the CSM network are subject to the provisions of this policy. Additionally, since Colorado law provides that E-mail communications written in the conduct of public business are generally considered to be public records, all E-mail communications written and sent in the conduct of public business by CSM employees are subject to applicable provisions of this policy, regardless of whether the communication was sent or received on a public or privately owned personal computer.

D. Application of Public Records Statutes to E-Mail

E-mail messages are subject to many of the same statutes and legal requirements as other forms of communication, such as the Colorado Open Records Act, §24-72-201, *et seq.*, C.R.S. (1997), which governs public access to CSM records, and the Archives and Public Records Act, §24-80-101, *et seq.*, C.R.S. (1997), which governs the retention, archiving, and destruction of CSM documents and records. The Open Records Act treats electronic documents and files in the same manner as paper documents. All such documents are generally considered to be public records and are subject to public inspection unless they are covered by a specific statutory exception. E-mail messages that are public records must be retained in either paper or electronic format. E-mail messages that are not public records should be

deleted after viewing. The Archives and Public Records Act requires that all documents pertaining to the business of CSM, whether in paper or electronic form, be retained, archived, or destroyed, as appropriate. Disposition decisions regarding individual documents should be made at the operational unit level with cognizance of the definition of public records and in accordance with CSM operating procedures. Although current CSM practice includes the daily back-up of central computer files, including some E-mail messages, such back-up is only undertaken for temporary storage purposes and is not intended to serve as a mechanism for archiving public records.

E. Privacy and Confidentiality

Even though E-mail users may intend their messages to be private communications between themselves and another party, the privacy and confidentiality of E-mail cannot be guaranteed by CSM for many reasons, including the following: E-mail messages may be saved indefinitely on the receiving computer, copies of E-mail messages can be made electronically or on paper, E-mail messages can be intentionally or accidentally forwarded to others, and messages may be sent to incorrect E-mail addresses or be improperly delivered by an E-mail system. Although CSM employees are permitted to use E-mail for personal communications, they should be aware that there are more appropriate avenues of communication available for matters requiring privacy or confidentiality.

F. Monitoring of E-Mail Communications by CSM

CSM does not intend to monitor E-mail usage by its employees in a regular or systematic fashion; however, it does reserve the right to monitor such usage from time to time and without prior notice. Such monitoring may include tracking addresses of E-mail sent and received, accessing in-box messages, accessing messages in folders, and accessing archived messages. E-mail monitoring which focuses on a specific individual or a selected group of individuals, must be based on a reasonable suspicion of misuse or wrongdoing and must be approved in advance by the appropriate vice president or the President. CSM may take corrective action or disciplinary action against an employee based upon information obtained from monitoring or inspecting his or her E-mail communications. Furthermore, CSM may disclose E-mail communications sent to, received by, or relating to an employee to law enforcement officials without giving prior notice to the employee.

G. Prohibited E-Mail Practices

Employees are prohibited from engaging in any of the practices described below on the CSM network. CSM may suspend or revoke the E-mail privileges of any employee who abuses them. Additionally, CSM may impose appropriate sanctions, ranging from reprimand to termination, upon an employee who engages in one or more of the following activities:

1. Sending obscene or patently offensive E-mail without the consent of the recipient;
2. Sending intimidating, threatening, harassing, or abusive E-mail;
3. Intercepting, disrupting, or altering an E-mail communication without proper authorization;
4. Accessing, copying, or modifying E-mail messages from or within the electronic files or records of another without permission;
5. Misrepresenting the identity of the source of an E-mail communication;
6. Allowing another to use one's E-mail account for fraudulent purposes;
7. Using E-mail to interfere with the ability of others to conduct CSM business;
8. Sending unsolicited "junk" E-mail or mass electronic mailings, such as chain letters, without a legitimate CSM business purpose;
9. Using E-mail for commercial purposes unrelated to CSM business;
10. Reproducing or distributing copyrighted materials without appropriate authorization; and
11. Using E-mail for any purpose which violates state law, federal law, or CSM policy.

Promulgated by the CSM Board of Trustees on May 7, 1998.