University of Colorado
Boulder • Colorado Springs • Denver

ADMINISTRATIVE POLICY STATEMENT

Policy Title: Use of Electronic Mail - #6002

POLICY DETAILS

Effective Date:	July 1, 1997
Responsible Office:	Assistant Vice President for Computing and Information Technology
Approved by:	Stuart M. Takeuchi
Application:	All Campuses
Replaces:	Use of Electronic Communications (dated March 1, 1996)

INTRODUCTION

The University provides electronic mail resources to support its work of teaching, scholarly research, and public service. This administrative policy statement sets forth the University's policy with regard to use of, access to, and disclosure of electronic mail to assist in ensuring that the University's resources serve those purposes.

STATEMENT OF POLICY

A. Privacy, Confidentiality and Public Records Considerations

The University of Colorado will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the University can assure neither the privacy of an individual user's use of the University's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

In addition, Colorado law provides that communications of University personnel that are sent by electronic mail may constitute "correspondence" and, therefore, may be considered public records subject to public inspection under Colorado's Public Records Act, C.R.S. 24-72-203.

B. Permissible Uses of Electronic Mail

1. Authorized Users

Only University faculty, staff, and students and other persons who have received permission under the appropriate University authority are authorized users of the University's electronic mail systems and resources.

2. Purpose of Use

The use of any University resources for electronic mail must be related to University business, including academic pursuits. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for the University.[1] Any such incidental and occasional use of University electronic mail resources for personal purposes is subject to the provisions of this policy.

C. Prohibited Uses of Electronic Mail

1. Prohibited Purposes

a. Personal use that creates a direct cost for the University is prohibited.

b. The University's electronic mail resources shall not be used for personal monetary gain or for commercial purposes that are not directly related to University business.

2. Other Prohibited Uses

Other prohibited uses of electronic mail include, but are not limited to

a. Sending copies of documents in violation of copyright laws

b. Inclusion of the work of others into electronic mail communications in violation of copyright laws.

c. Capture and "opening" of electronic mail except as required in order for authorized employees to diagnose and correct delivery problems.

d. Use of electronic mail to harass or intimidate others or to interfere with the ability of others to conduct University business.

e. Use of electronic mail systems for any purpose restricted or prohibited by laws or regulations.

f. "Spoofing," i.e., constructing an electronic mail communication so it appears to be from someone else.

g. "Snooping," i.e., obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial University business purpose.

h. Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.

D. University Access and Disclosure

1. General Provisions

a. To the extent permitted by law, the University reserves the right to access and disclose the contents of faculty, staff, students', and other users' electronic mail without the consent of the user. The University will do so when it believes it has a legitimate

business need including, but not limited to, those listed in paragraph 3 (below), and only after explicit authorization is obtained from the appropriate University authority.

b. Faculty, staff, and other non-student users are advised that the University's electronic mail systems should be treated like a shared filing system, i.e., with the expectation that communications sent or received on University business or with the use of University resources may be made available for review by any authorized University official for purposes related to University business.

c. Electronic mail of students may constitute "education records" subject to the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974 (FERPA). The University may access, inspect, and disclose such records under conditions that are set forth in the statute.[2]

d. Any user of the University's electronic mail resources who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under appropriate University authority.

2. Monitoring of Communications

The University will not monitor electronic mail as a routine matter but it may do so to the extent permitted by law as the University deems necessary for purposes of maintaining the integrity and effective operation of the University's electronic mail systems.

3. Inspection and Disclosure of Communications

The University reserves the right to inspect and disclose the contents of electronic mail:

- in the course of an investigation triggered by indications of misconduct or misuse,
- as needed to protect health and safety,
- as needed to prevent interference with the academic mission, or
- as needed to locate substantive information required for University business that is not more readily available by some other means.

The University will inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfill the University's obligations to third parties.

4. Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring

The contents of electronic mail communications, properly obtained for University purposes, may be disclosed without permission of the user. The University will attempt to refrain from disclosure of particular communications if disclosure appears likely to create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

5. Special Procedures to Approve Access to, Disclosure of, or Use of Electronic Mail Communications

Individuals needing to access the electronic mail communications of others, to use information gained from such access, and/or to disclose information from such access and who do not have the prior consent of the user must obtain approval in advance of such activity from the appropriate University authority. The Chancellor of each campus shall develop a written statement of procedure to be followed to request such approval. That

procedure shall take into consideration ways to minimize the time and effort required to submit and respond to requests, the need to minimize interference with University business, and protection of the rights of individuals. A list of guiding concepts and a template for such a procedure is provided as Attachment A.

E. Disciplinary Action

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of the University's electronic mail resources.

F. Public Inspection, Retention, and Archiving of Electronic Mail

1. Public Inspection of Electronic Mail

Communications of University employees in the form of electronic mail may constitute "correspondence" and therefore may be a public record subject to public inspection under C.R.S. 24-72-203 of the Colorado Public Records Act.

2. Retention and Archiving of Electronic Mail

Electronic mail messages produced or stored using state-owned equipment or software generally are excluded from the definition of "records" subject to the provisions of the State Archives and Public Records Act, C.R.S. 24-80-101, et seq.

Note, however, that if the recipient of electronic mail messages has previously segregated and stored such messages as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the University or because of the value of the official University data contained therein, then such messages must be retained, archived, and destroyed in compliance with the relevant portions of the State Archives and Public Records Act.

---

[1] An example of a use that does not create a direct cost is sending an email message during an employee's lunch hour: the University will pay no more for maintaining the email system than it would have paid had the message not been sent. An example of a use that does create a direct cost is printing an email message without reimbursing the University.

[2] Students who are also employees of the University should be given the opportunity to have separate accounts for their employment-related electronic mail to insulate their student communications from inadvertent disclosure.

ATTACHMENT A

Concepts and Template for Granting Approval to Access Electronic Communications of Others

The following are suggestions for elements to be considered in designing the process for granting approval to access electronic communications addressed to others:

1. What information is needed to determine whether a request should be approved? Possibilities include:

* Name and title of the person whose communications will be accessed;

* Name and title of the person who will do the accessing;

* Why the access is needed;

* What forms of communication will be accessed (e.g., voice mail, E-Mail, FAX);

* Required duration of the access;

* What will be done with the accessed messages? With whom will they be shared?

2. Who should be able to request access? Who should be able to approve requests? Possibilities include:

* Department Chairpersons and Unit Directors should be able to request access;

* Deans or Vice Chancellors should be able to approve requests.

3. Who needs to be informed when a request is approved to implement the access? The approved request must be routed to those people who should keep a copy of the request.

4. What advice or reminders should be given to the person requesting the access? Possibilities include:

* A reminder that concerns about fiscal misconduct or criminal activity should not be investigated by individuals or departments but should be referred to University Police or Internal Audit staff in accordance with the University Administrative Policy titled "Reporting Fiscal Misconduct."

* A reminder that the contents of electronic communications obtained after appropriate authorization may be disclosed without the permission of the employee. At the same time, the University will attempt to refrain from disclosure of particular messages if disclosure could create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

A sample access request form is attached.

REQUEST TO ACCESS ELECTRONIC COMMUNICATIONS OF OTHERS

Our department requests authority to access electronic communications sent to an individual as described below:

1. Name, Title, and Department of person whose communications would be accessed:

_____

Name & Title

_____

Department

2. Name, Title, and Department of person who will do the accessing:

_____

Name & Title

_____

Department

3. Reason for access request:_____

_____

_____

_____

4. What forms of communication will be accessed (e.g., voice mail, E-Mail, FAX)

_____

_____

5. How long should the special access last? _____

_____

6. What will be done with the accessed messages? With whom will they be shared?

_____

_____

_____

7. _____

Signature of Requesting Department Chairperson or Unit Director

_____

Date

8. _____

Signature of Approving Dean or Vice Chancellor

_____

Date

9. Upon approval, this form is to be delivered to the following person as authorization for them to implement the requested special access.

_____

Name & Title

_____

Department