University of Colorado **Denver | Anschutz**

Campus Administrative Policy

Policy Title: Email

Policy Number: 5011 Functional Area: Information Technology

Effective:	December 11, 2020
Date Last Reviewed:	December 11, 2020
Date Scheduled for Review:	July 1, 2027
Supersedes:	Email (September 1, 2012, January 21, 2003)
Approved by:	Donald M. Elliman, Jr. Chancellor, University of Colorado Anschutz Michelle A. Marks Chancellor, University of Colorado Denver
Prepared by:	Legal & University Communications
Reviewing Office:	Executive Vice Chancellor for Finance and Administration | CFO, CU Anschutz Senior Vice Chancellor for Finance and Administration | CFO, CU Denver
Responsible Officer:	Chief Information Officer
Applies to:	CU Anschutz CU Denver

A. Introduction

University of Colorado Denver | Anschutz ("the university") considers information technology a strategic asset that is relied upon by faculty, staff, and students to accomplish the university mission. As such, the use of electronic mail (email) and the protection of information contained within the university email system is critical to the success of the university. This policy applies to all users of the university email systems, including students, faculty, and staff.

Email is one of the most powerful and commonly used communication tools within the university, but there are many risks associated with communicating via email. Email communications should not be considered to be confidential exchanges of information, as they can be viewed by anyone unless properly protected. Email messages can also be intercepted, stored, read, modified, and/or forwarded to other recipients. In addition to these security concerns, casual comments in email may be misinterpreted and lead to contractual or other legal issues for staff and faculty.

B. Policy Statement

1. Purpose

   University email services are provided to support the academic, business and research missions of the university. All emails processed by the university information technology systems and networks are considered to be the property of the university.

2. Responsibility

   Email users are responsible for avoiding practices that could compromise information security. This includes (but is not be limited to) preventing unauthorized access to email accounts by properly protecting login credentials, not storing passwords on public-access systems and proper use of encryption services for sending private data.

3. Email as Official Communication

   Email is an official means of communication within the university. Therefore, the university has the right to send communications to students, faculty and staff via email, and the right to expect that those communications will be received and read in a timely fashion.

4. Expectations

   Students, faculty, and staff are expected to check their official email address on a frequent and consistent basis in order to stay current with university communications. Students, faculty, and staff have the responsibility to recognize that certain communications may be time critical. University e-mail is provided

to support University activities and excessive personal use should be avoided.

5. Encryption

   Data that is classified as Private (as defined in the CU System Policy Glossary, see references, below) must be encrypted when being sent to recipients outside of the university and its affiliates' networks (i.e. when sent across the Internet or other public networks.). Such emails must be encrypted through an IT Services-managed encryption system.

6. Out of Office Messages

   Do not unnecessarily disclose potentially sensitive information in "out of office" or "automated reply" messages (reference Email Security Guidelines, below).

7. Privacy

   IT Services reserves the right to scan email traffic for malicious software, spam and unencrypted private or restricted information. While the university encourages the use of electronic mail and respects the privacy of users, all emails traversing university computing systems and networks are subject to automated scanning and monitoring. Emails may also be quarantined and/or reviewed by authorized university employees.

8. Interception/Modification

   Except when specifically authorized by university management or where necessary for IT system administration purposes, employees must not intercept, divert, modify, or destroy another person's email communications or messages.

9. Personal Use of University Email Accounts

   University email services may be used for incidental personal purposes provided that such use does not: (i) directly or indirectly interfere with the operation of computing facilities or electronic mail services; (ii) burden the university email system with noticeable incremental cost; or (iii) interfere with the email user's employment or other obligations to the university. Email messages arising from such personal use are also considered to be the

property of the university with no expectation of privacy. Email users should assess the implications of this presumption in their decision to use university electronic mail services for personal purposes.

10. Personal Email Accounts

    Use appropriate discretion when using Gmail, Hotmail, Yahoo or any similar external/third-party email services for university business or academic purposes. Do not forward or auto-forward university email that may contain private or restricted data (e.g. PHI, SSNs, or FERPA-protected data) to external/third party email systems or store such email data on insecure mobile devices.

11. Distribution lists and Listservs

    Exchange/Outlook email distribution lists should ONLY be used for email communications being sent to less than 150 recipients. Larger volumes of messages should be processed through IT Services managed listservs or other IT Services- approved email tools. IT Services provides free listserv services for faculty & staff.

12. Campus-wide Distribution

    Only the Chancellor, the President, or their designee may send email communications to the entirety of the university. This includes faculty and/or staff and/or student populations.

13. Restrictions

    Do NOT use email:

    a. To create, send, forward or store emails with messages or attachments that are illegal or violate any other campus or University policy.

    b. To commit the university to a third party, for example through purchase or sales contracts, job offers or price quotations, unless you are explicitly authorized by management to do so (principally applies to staff within the

       Procurement Service Center and Human Resources)

    c. In ways that could be interpreted as representing or being statements on behalf of the university, unless you are a

spokesperson explicitly authorized by university management to make such statements.

d. To send a message from anyone else's email account or in their name (including the use of false or spoofed 'From:' addresses). If authorized by their manager, administrative assistant or other office personnel may send email on the manager's behalf but should sign such email in their own name per procuration ('for and on behalf of') the manager.

C. Responsible Organization

1. Information Strategy and Services is responsible for interpretation and guidance regarding this policy.
2. The Office of Regulatory Compliance is responsible for campus compliance and enforcement of this policy.

D. Procedures

Violation of this policy or other university information technology policy can result in revocation of computing privileges as well as corrective and/or disciplinary action.

Notes

1. Dates of official enactment and amendments:
   September 21, 2003: Adopted by Vice Chancellor for Administration and Finance September 1, 2012: Revised
   March 11, 2020: Reviewed—no changes
   December 11, 2020: Revised, Adopted by the Chancellors

2. History:
   January 18, 2019: Modified to reflect a Campus-wide effort to recast and revitalize Campus policy sites into a standardized and more coherent set of chaptered policy statements organized around the several operational divisions of the university. Article links, format, and University branding updated by the Provost's office.
   December 11, 2020: Revised to clarify e-mail uses.
   March 2026: Updated campus and office naming.

3. Initial Policy Effective Date: September 21, 2003

4. Cross References/Appendix:
   - CU System Administrative Policy 6002, Electronic Communications
   - CU System Policy Glossary
   - Campus Administrative Policy 5005, Information Systems Networked Resource Passwords
   - Campus Administrative Policy 5001, Acceptable Use of Information Technology Resources
   - Local Network Access Policy
   - Remote Access Policy
   - Email Security Guidelines
   - HIPAA Regulations
   - FERPA Regulations