University of Colorado
Denver | Anschutz Medical Campus

Campus Administrative Policy

Policy Title: Email

Policy Number: 5011 Functional Area: Information Technology

Effective:	September 1, 2012
Date Last Amended/Reviewed:	September 1, 2012
Date Scheduled for Review:	July 1, 2019
Supersedes:	Email (January 21, 2003)
Approved by:	Vice Chancellor for Administration and Finance
Prepared by:	Office of Information Technology
Reviewing Office:	Office of Information Technology
Responsible Officer:	N/A
Applies to:	University of Colorado Anschutz Medical Campus University of Colorado Denver

---

A. INTRODUCTION

University of Colorado Denver | Anschutz Medical Campus (the) 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 defines the appropriate use of email and the university email system. 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.

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.

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. **Etiquette and Discretion**
Apply appropriate and reasonable discretion when using email, for example abiding by the generally accepted rules of email etiquette (reference Email Security Guidelines, below). Review emails carefully before sending, especially formal communications with external parties.

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

8. **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.

9. **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.

10. **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 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.

11. **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.

12. **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 and staff.

13. **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.

14. **Restrictions**
Do NOT use email:
   a. To create, send, forward or store emails with messages or attachments that might be illegal or considered offensive by an ordinary member of the public. (e.g., sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive).
   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 official public 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, an administrative assistant or other office personnel may send email on the manager's behalf, but should sign such email in their own name per pro ('for and on behalf of') the manager.
e. To send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, color, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters and hoaxes, charity requests, viruses or malicious software.
f. For any other illegal, unethical or unauthorized purpose.

C. RESPONSIBLE ORGANIZATION

1. Information Technology 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

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 statement organized around the several operational divisions of the university. Article links, format, and University branding updated by the Provost's office.

3. Initial Policy Effective Date: September 21, 2003

4. Cross References/Appendix:
   - CU System APS: Email

- CU System Policy Glossary
- Information Security Policy
- Campus Policy 5001, *Acceptable Use of Information Technology Resources*
- Local Network Access Policy
- Remote Access Policy
- Email Security Guidelines
- HIPAA Regulations
- FERPA Regulations