

UNIVERSITY POLICIES

A GROWING CATALOG OF COLUMBIA-WIDE POLICIES

[Home](#) » [Email Usage Policy](#)

Email Usage Policy

Provides guidance for: proper use of email, necessary actions for sending sensitive data via email and privacy expectation

▼ Overview

I. Introduction

Email is an expedient communication vehicle to send messages to the Columbia University community. The University recognizes and has established the use of email as an official means of communication. However, use of an email system at the University requires adequate security measures to protect the University Data (as such term is defined in the Columbia University [Information Security Charter](#) (the “Charter”)) that is transmitted.

Capitalized terms used herein without definition are defined in the Charter.

II. Policy History

The effective date of this Policy is November 1, 2013. This Policy and other Information Security Policies replace (A) the following University Policies:

- Electronic Information Resources Security Policy, dated March 1, 2007
- Email Usage and Retention Policy, dated April 1, 2008

and (B) the following CUIMC Policy:

- Communicating Protected Health Information via Electronic Mail (Email) at Columbia University Medical Center, dated January 21, 2004, and amended as of September 21, 2012

▼ Policy Text

III. Policy Text

A. Approved University Email Systems

All email used to conduct University business must be transmitted via an Approved University Email System. For purposes of this Policy, an “Approved University Email System” is Lionmail, any CUIT or CUIMC IT Email System and any other Email System that has been risk assessed and approved by the applicable Information Security Office.

B. Prohibited Actions

No User of University email may take any of the following actions:

1. Send or forward an email through a University System or Network for any purpose if such email transmission violates laws, regulations or University policies and procedures;
2. Use any Email System other than an Approved University Email System to conduct University business or to represent oneself or one’s business on behalf of the University. Examples of Email Systems that are not approved include a personal email account or a personal Columbia Alumni Association account (i.e., anything@caa.columbia.edu).
3. Send nuisance email or other online messages such as chain letters;
4. Send obscene or harassing messages;
5. Send unsolicited email messages to a large number of Users unless explicitly approved by the appropriate University authority; or
6. Impersonate any other person or group by modifying email header information to deceive recipients.

C. Provisions Relating to Emails Containing Sensitive Data

Each User shall ensure that Sensitive Data is transmitted by email only if the following conditions are met:

1. Except as provided in Section D below, all email communications of Sensitive Data are encrypted before being transmitted.
2. Sensitive Data are not transmitted in the “Subject” line of an email.
3. Before transmitting an email that contains Sensitive Data, the User verifies that no unintended information is included in the message or any attachment and that the proper document is attached.
4. Before transmitting an email that contains Sensitive Data, the User verifies the names and email addresses of the intended recipients.

D. Provisions Relating to Email Within the Columbia Health Care Component

For purposes of this Policy, an “Approved OHCA Email System” is any CUIT Email System other than Lionmail, any CUIMC IT Email System and any other Email System used within the CUIMC/Hospital OHCA that has been approved by the CUIMC Information Security Office.

The following provisions relate only to email transmitted by Users within the Columbia Health Care Component:

1. Unencrypted EPHI may be transmitted internally if sent on an Approved OHCA Email System.
2. No automatic forwarding, redirection or automated delivery of email outside the CUIMC/Hospital OHCA may be used.