

# **Email Usage & Retention Policy**

**Effective Date: April 1, 2008**

## **Policy Statement**

Email is an expedient communication vehicle to send messages to the Columbia University population. Because of the versatility and ubiquity of email technology, Columbia University recognizes and has established the use of email as an official means of communication. University email includes Cubmail, Outlook, and other specific services offered by the Business School, Law School and Columbia University Medical Center. This policy defines the appropriate use of Columbia University's email and its retention.

## **Primary Guidance to Which This Policy Responds**

This policy responds to the "Acceptable Use of IT Resources" and the "Desktop and Laptop Security" policies.

## **Responsible University Office & Officer**

The office of Columbia University Information Technology Security is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Chief Information Security Officer (CISO) is the responsible officer.

## **Revision History**

This policy was established in April 2008.

## **Who is Governed by This Policy**

This policy applies to all individuals who are granted a Columbia University email account. A Columbia University email is defined as [insert definition?] Those individuals covered include, but are not limited to, faculty, staff, students, those working on behalf of the University, and/or individuals authorized by affiliated institutions and organizations.

## **Who Should Know This Policy**

Anyone with a Columbia University email account should know this policy.

## **Exclusions and Special Situations**

None

## **Policy Text**

The following lists the acceptable use and security measures that one must exercise when using Columbia University's email.

1. Messages sent and received via Columbia's email system should be kept as private as possible by senders and recipients, as well as by Columbia University Information Technology (CUIT). The University and its email system administrators will not read email unless necessary in the course of their duties (e.g., including investigation, inappropriate contents or as directed by Office of the General Counsel, and will release email as required by an executed subpoena valid in the State of New York).

2. No email may be sent or forwarded through a University system or network for purposes that violate University statutes or regulations or for an illegal or criminal purpose.
3. When conducting University business, only a Columbia University email account (e.g., UNI@columbia.edu, name@columbia.edu, anything@columbia.edu, name@gsb.columbia.edu, or name@law.columbia.edu) is acceptable for official University and/or business related correspondences. The use of personal email accounts, to conduct such University business, including personal Columbia Alumni Association accounts (anything@caa.columbia.edu), to represent oneself or one's enterprises on behalf of the University is prohibited.
4. Nuisance email or other online messages such as chain letters or obscene, harassing, offensive or other unwelcome messages are prohibited. Such email should be reported to the departmental system administrator or CUIT help desk immediately.
5. Unsolicited email messages to multiple users are prohibited unless explicitly approved by the appropriate University authority. See <http://www.columbia.edu/cu/policy/mass-email-procedure.html>
6. Confidential and/or sensitive information (e.g., SSN, credit card, medical records) must not be sent by email. The only acceptable way to transmit such information electronically is to attach the information as a password-protected and/or encrypted file; never type the information in the body of the email; and never send a password or decryption key in the same email. Unless the file is encrypted or password-protected, it can be read by others and therefore should not be considered private communication.

Instructions for password protecting and encrypting Microsoft Office documents can be found at <http://www.columbia.edu/acis/security/articles/data/encryption.html>

For communications involving health care and medical information, you must adhere to the Columbia University Medical Center's email policies. Please see:

<http://www.cumc.columbia.edu/hipaa/policies/docs/cumcemailpolicy.pdf>

[http://www.cumc.columbia.edu/hipaa/policies/docs/cumcimptinfo\\_provider.pdf](http://www.cumc.columbia.edu/hipaa/policies/docs/cumcimptinfo_provider.pdf)

Prior to sending an email with sensitive and/or confidential information, verify the accuracy of the recipient's email address to prevent unintentionally sending it to an unauthorized individual. Once an email is sent, it cannot be recalled and /or undone.

7. All messages must show the genuine sender information (i.e., from where and from whom the message originated). Users are not allowed to impersonate other users or user groups, real or fabricated, by modifying email header information in an effort to deceive the recipient(s); e.g., email spoofing is specifically prohibited.

8. Potentially damaging emails (e.g., unsolicited, mass or commercial messages; messages that appear to contain viruses) will disrupt University operations. To prevent the spread of this type of email, the University reserves the right to terminate its connection to outside host servers, as well as filter, refuse and/or discard these messages.
9. Email boxes that are hosted on CUIT servers are backed up nightly and retained for up to five weeks. Deleted and purged email, if available in a backup copy, may be recoverable if the request is not longer than five weeks from the date of deletion. Email forwarded (i.e., redirected) to a personal email account (e.g., Gmail, Yahoo, Hotmail) that is not under CUIT control is excluded from the CUIT email backup.

### **Responsibilities**

The intentional abuse of email privileges may result in having your University email account suspended / revoked. Unauthorized access to read another person's email will be treated with the utmost seriousness, including disciplinary actions, suspension and/or termination.

### **Definitions**

*Deleted and purged email* – When an email is deleted, it is flagged for deletion and remains on the system; at this point, the message can still be undeleted by restoring it from the Trash. Once a deleted message is purged from the system (e.g., via a "purge" command, emptying the Trash or by using the "Erase Deleted Messages" command), the message is generally retained online for about a week; administrators can access it, but is no longer counted against the owner's quota.

### **Contacts**

For questions or comments:

Columbia University Information Technology

Web: <http://www.columbia.edu/cuit/support/>

Email: [security@columbia.edu](mailto:security@columbia.edu)

Telephone: 212-854-1919

### **Cross References to Related Policies**

For CUIT Security Policies, see the University Administrative Policy Library, CU Information Technology section:

[http://www.columbia.edu/cu/administration/policylibrary/responsible\\_office/cuit.html](http://www.columbia.edu/cu/administration/policylibrary/responsible_office/cuit.html)

For additional policies relating to computing use, computer security standards and guidelines, data classification and encryption, see the “Acceptable Use of IT Resources”, “Desktop and Laptop Security”, “Data Classification” and “Encryption” policies.

For Columbia University Student Email policy, see:

<http://www.columbia.edu/acis/history/cu-email.html>

For Columbia University Medical Center's email policies, see:

<http://www.cumc.columbia.edu/hipaa/policies/docs/cumcemailpolicy.pdf>

[http://www.cumc.columbia.edu/hipaa/policies/docs/cumcimptinfo\\_provider.pdf](http://www.cumc.columbia.edu/hipaa/policies/docs/cumcimptinfo_provider.pdf)

For Columbia Law School's email policy, see:

[http://www.law.columbia.edu/law\\_school/info\\_tech/Fac\\_Sup/policies?#rtregion:main](http://www.law.columbia.edu/law_school/info_tech/Fac_Sup/policies?#rtregion:main)

For Columbia Business School's email policies, see:

[http://www0.gsb.columbia.edu/itg/students/policies\\_resources/emailsupport](http://www0.gsb.columbia.edu/itg/students/policies_resources/emailsupport)

<http://www0.gsb.columbia.edu/itg/admin/security/Email>

[http://www0.gsb.columbia.edu/itg/EmergingTech/Mail\\_Protection](http://www0.gsb.columbia.edu/itg/EmergingTech/Mail_Protection)