

E-mail Archiving Frequently Asked Questions (FAQs)

Question 1: Does the deletion from the archive after one year mean that my emails will no longer be available in my Union email account?

Answer. No. Emails in your Union email account will not be deleted unless you delete them. The email archive is a separate system. Your Union email account will function as it always has. Emails will be saved permanently unless you delete them.

Question 2: Will every email I have already sent now be archived as of August 24?

Answer. Emails sent or received before August 24, 2009 will not be archived.

Question 3: If I forward my email messages that are addressed to me at “username@union.edu” to an account at AOL, hotmail, juno or another external email account will the messages be accessible to Union College?

Answer. Email messages that are addressed to “username@union.edu” are first received by the Union email system before they are routed to your [AOL, hotmail, juno, gmail, etc.] external account (e.g. “username@AOL.com”). Thus, they would be archived by Union at the secure vendor site for one year, and they will be deleted from the archive after 12 months.

If you compose and send your messages from your [AOL, hotmail, juno, gmail, etc.] external account and do not route them through your union.edu email account, they will not be archived. Any email that you compose and send directly from your union.edu email account will be archived. Also, any email received by a union.edu email account will be archived.

If your work-related emails were subpoenaed and you had sent them using a non-Union email account, they would still be subject to the subpoena.

Question 4: Is the wholesale storage of ALL e-mail messages mandated by law, and/or by any other directive/decreed/finding, etc?

Answer. The new Federal Rules of Discovery require a party to suspend routine or intentional purging, overwriting, reusing, deleting, or any other destruction of electronic information relevant to a dispute but only upon notice to that party that a lawsuit has been commenced against it or upon reasonable anticipation that a lawsuit may be brought. This electronic information must be preserved so that it can be retrieved – if necessary – at a later time. The information must be preserved in its original electronic form, so that all information contained within it, whether visible or not, is also available for inspection – i.e., it is not sufficient to make a hard copy of electronic communication. Since Union College’s email services are not able to retrieve emails in a timely fashion or cost effective manner, contracting with Google to archive electronic mail off-site allows the College to satisfy its legal obligations under the Federal Rules of Discovery. Failure to produce subpoenaed emails has resulted in million dollar lawsuits against companies.

Question 5: E-mail could contain sensitive (third-party related) material, e.g., tenure-committee related, student advising material, etc. What happens to privacy rights issues? Can IT read my emails?

Answer. In the context of a discovery demand, it is important to understand that, although the information must be preserved, no data will be disclosed to the opposing party without first being

appropriately reviewed to determine legal necessity and relevancy and to remove legally privileged information. In other words, personal and other irrelevant information and privileged documents (e.g., attorney-client communications) will not be disclosed to the opposing party.

Additionally, it is important to stress that the Security and Privacy provisions found in the College's *Responsible Use of Union College Computing and Network Services Policy* (reprinted below), that has been in effect since September 2006, will apply to archived electronic mail.

In accordance with College policy, Union ITS employees do not read your emails (nor will they read emails that are archived), unless reasonable cause to believe a legal or policy violation has occurred that may require monitoring. In this event, the decision to read emails will be made on a case-by-case basis. However, the Chief Information Officer must authorize the decision to monitor emails (except as required by law or necessity to respond to emergency situations). It is common practice by the Chief Information Officer to relinquish decision-making responsibility regarding monitoring emails to the appropriate Vice President and/or the President. Since its adoption and implementation in September 2006, the Security and Privacy Policy has proven effective in addressing privacy concerns.

From the Union College Faculty Manual (FM Section VI - Sundry Matters, XIV, p. 33); Student Handbook 2008-2009 (page 99):

Security and Privacy

Union College employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the College cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users should also be aware that their uses of College computing resources are not completely private. While the College does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the College's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, the scanning of systems and network ports for anomalies and vulnerabilities, and other such activities that are necessary for the rendition of service. The College may also specifically monitor the activity and accounts of individual users of College computing resources, including individual login sessions and communications, without notice, when:

- a. the user has given permission or has voluntarily made them accessible to the public, for example by posting to a publicly-accessible web page or providing publicly-accessible network services;
- b. it reasonably appears necessary to do so to protect the integrity, security, or functionality of the College or other computing resources or to protect the College from liability;
- c. there is reasonable cause to believe that the user has violated, or is violating, this policy;
- d. an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or

- e. it is otherwise required or permitted by law. Any such individual monitoring, other than that specified in “(a)”, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer or the Chief Information Officer’s designees.

Union College, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate College personnel or law enforcement agencies and may use those results in appropriate College disciplinary proceedings.

Question 6: Is spam/junk mail (say addressed to me without my consent) archived as well?

Answer. E-mail that is not caught by the SPAM filter (and put into quarantine) will be archived. Also, if you release e-mail from Quarantine and have it delivered, it will be archived.

Question 7: Can the third-party vendor (in this case Google) be required by law (or by directive, decree, etc.) to disclose Union e-mail regardless of Union's consent, and/or the faculty member's consent? And/or regardless of Union, and/or the faculty member, being informed of such action?

Pursuant to the contract the College has with Google:

Union College and Google will (a) protect the other party’s Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to affiliates, employees, and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any affiliates, employees, and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill obligations under the Agreement, which using reasonable care to protect it. Each party is responsible for any actions of its affiliates, employees, and agents in violation of the Agreement.

Union College and Google may disclose the other party’s Confidential Information when required by law but only after it, if legally permissible, (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

Question 8: Who has access to the archive and on what basis? Directive?

Answer. The Chief Information Officer (CIO) of the College. As noted above, under response to Question 5, access will only be made on the basis of a legal directive (subpoena, court order, etc.) or with the approval of a member of the President’s staff. In the case of a legal directive, the CIO will consult with the College Attorney before any action is taken.

Question 9: Is this a homeland security directive?

Answer. No. E-mail archiving is being undertaken so that the College can meet the requirements of a discovery demand if one is ever required.