

Colby College Electronic Mail Policy and Procedures

Principles, Policies, User Responsibilities, and Information Technology Services (ITS) Operational Procedures

- (1) **Electronic mail is an important medium for communication, both on the Colby campus and with those elsewhere on the world-wide network.**

Use of this medium by students, faculty, and staff is encouraged for scholarly, work-related, and personal communication within the constraints of ethical standards and other policies, procedures, and job responsibilities that are in place at Colby.

- (2) **Electronic mail is private and owned by the sender and each recipient account holder.**

The use of each account is the personal responsibility of the account holder. The contents of electronic mail will not be monitored, censored, or otherwise examined except with specific authorization and direction by the appropriate Dean or Vice President or as part of the required system administration as described below.

- (3) **Court order or law enforcement investigation may require the examination and release of any document, including electronic files such as e-mail.**

When a person affiliated in any way with the College is involved, ITS will act only under the specific instructions of a member of the Senior Staff to ensure that individual rights, including rights to privacy and due process, are maintained.

- (4) **Colby staff members may, under certain conditions, have e-mail files accessed by others when it is related to departmental functions.**

A special condition exists for a staff employee who receives mail associated with his/her job responsibilities and where, in their absence, the supervisor or others in the department need to have access to the mail. ITS must continue to maintain the privacy of mail but, on authorization from the department head, may locate and copy specific messages; no person outside ITS may review the entire contents of an account's system mailbox without authorization of an appropriate Dean or Vice President.

- (5) **Mail moved by the account holder outside the mail systems becomes personal files covered by other policies and procedures.**

Note that mail downloaded to files using Eudora or other application on a personal computer or saved to files on a minicomputer is covered by other policies and procedures. Those files on a personal computer are outside the system management of ITS. Maintenance of e-mail privacy is controlled, at least to a great extent, by permitted access to the personal computer, which is the responsibility of the individual.

- (6) **ITS administers the campus electronic mail system in a manner consistent with the system's importance for campus communication and the need for privacy of e-mail messages.**

In the process of administering the electronic mail system, certain members of the ITS staff may have access to the contents of certain e-mail messages. The ITS staff members will exercise their ability to access the contents of e-mail under the strict limitations of the system administration requirements (a "need to know" basis). Furthermore, information about the contents of e-mail obtained by members of the staff as they administer the e-mail system must not be communicated to other members of the ITS staff unless required to administer and support the system, and may not be communicated to anyone outside ITS without the approval of the appropriate Dean or Vice President (with the exception noted in (4) above).

- (7) **The electronic mail system operates in a best effort manner to deliver messages as specified by the sender, protecting the privacy of the contents.**

Although highly reliable and secure, delivery to on-campus e-mail addresses is not guaranteed, there can be no assurance that the person holding the recipient account actually examines a particular message, nor can confidentiality be absolutely guaranteed. In all these respects, electronic mail is no different from campus mail. ITS can provide advice on how to use additional procedures and software with the system when higher levels of security and confirmed delivery are required.

(8) There are no assurances about the handling of e-mail received from or sent to addresses outside Colby.

Organizations managing e-mail systems elsewhere on the network may or may not have similar policies to those described here. Many are known to consider e-mail the property of the organization, subject to examination. Be aware of this possibility when you correspond with those elsewhere on the network. While ITS may be able to provide some advice, Colby has no direct influence on the handling of e-mail anywhere outside the local network.

(9) Some information about personal mail use is not confidential because of the way computer systems operate.

Depending on how a person uses e-mail, the following information can be seen by other people:

- The fact that a person is running a mail application.
- The account to which mail is being addressed (true only on a UNIX system such as a HP computer and only under certain circumstances).
- The size of the account's mailbox (mail waiting to be read).
- The date and time mail was last read.

(10) The administrators of Colby's e-mail facility may, within certain limits, block mail (including external, unsolicited, bulk e-mail –"spam").

The annoying, potentially resource intensive, and sometimes offensive nature of unsolicited bulk e-mail being sent by commercial or quasi-commercial organizations may require Colby's e-mail administrators to block receipt of mail from some locations on the Internet. This blocking action is permitted if justified and where such blocking minimizes the likelihood that legitimate e-mail to Colby account holders will be blocked as well. E-mail administrators are not permitted to use the content of the message or of the subject line in the mail heading to block or divert delivery of any message, except to block e-mail containing computer viruses or similar destructive content.

(11) The account holder must maintain password security.

Electronic mail addressed to an account is delivered to a mailbox file that can be accessed through a variety of computer programs (e.g., HP mail, Eudora) under account password control. The account holder is responsible for maintaining strict confidentiality of that password, as described in the general statement on computer ethics and responsibilities.

(12) The account holder is expected to manage all mail delivered to that account.

It is the responsibility of the account holder to manage her/his e-mail by suitably disposing of mail in the account's mailbox (deleting messages, transferring messages to a personal computer's storage such as with Eudora, or saving messages to files in the account's home directory on the minicomputer system). Managing e-mail also requires account holders to suitably control the automatic delivery of messages from such services as mailing lists (e.g., Listserv and Comserve).

(13) Electronic storage for mailboxes is limited and the ITS staff must ensure that sufficient space is available for the on-going delivery of new messages.

ITS will establish a maximum permissible mailbox size. When this size is exceeded, the entire mailbox contents may be moved to a new file in the account's home directory on the minicomputer, where it will be accessible by the account holder. An e-mail message notifying the account holder that this action has been taken will immediately be sent, thereby placing in the vacant or nearly vacant mailbox information about where other mail has been placed.

(14) E-mail messages will be deleted from the server 30 days after being read by the recipient.

It is possible for account holders to leave their e-mail on the server even after it has been read or otherwise downloaded, for example to Eudora on a personal computer. E-mail that accumulates in this manner creates both storage problems and processing delays. Any message that has been read or downloaded to a personal computer will be eligible for deletion 30 days later. No archive of this e-mail will be created. Unread, non-downloaded e-mail will not be deleted.

(15) The accumulation of a large volume of mail in an account's mailbox may require ITS to take management action.

A large volume of unread mail being received by an account can cause network and mail performance problems, in addition to storage problems, with no benefit to anyone. In cases where,

over a period of a week or longer, an account is receiving a large volume of mail and the account holder is not moving it out of the mailbox, ITS will implement stages of response to safeguard the account holder's mail, protect performance of the e-mail system, and help the account holder gain control over the amount of mail being received. These are the response stages:

(a) Whenever the mailbox is moved to a file in the account's home directory, an informational message sent by ITS will offer assistance and advice on how to manage the inflow of mail. It will alert the account holder to the need for him/her to take action in managing the account.

(b) ITS will contact the person by phone or conventional mail to alert them to the problem and request that immediate action be taken, offering advice on how to proceed.

(c) ITS will request permission from the appropriate Dean or Vice President to inactivate the account.

(16) Extraordinary action may be required under specific constraints.

Certain circumstances may require ITS to take extraordinary action in administering the e-mail system. This might be caused by such things as system malfunction or malicious actions by an individual. ITS must take steps to

(a) protect the privacy of mail,

(b) protect the functionality of the electronic mail system,

(c) protect account holders from disruption of their use of the electronic mail system.

Extraordinary action taken by ITS to limit an individual's access to the system or to inspect and/or alter the contents of a mailbox is subject to review by the appropriate Dean or Vice President.

(17) This policy should be reviewed annually or more often as needed.

Approved by the Information Technology Committee on May 5, 2009