

Skidmore College
Information Technology
Policy
Custodianship of Electronic Mail
April 27, 2010

The framework on which this work is based was provided in part by the Cornell University IT Policy Office and its Director Tracy Mitrano, and is gratefully acknowledged.

Custodianship of Electronic Mail

Contents

Document Statement	2
Principles	2
Reason for Document	2
Entities Affected by this Document	2
Who Should Read this Document	2
Website Address for this Document	2
Document Specifics	3
Procedures	3
Requests to Disclose the Content of Email	3
Local Support Providers: Usual Course of Business	5
Reporting Alleged Violations	5
Responsibilities	6
Definitions	8
Contacts	9
Related Documents	10

Custodianship of Electronic Mail

Document Statement

Skidmore administers an electronic mail (email) system, which it must manage for the entire college community in a manner that preserves a level of privacy and confidentiality while in accordance with relevant State and Federal laws, regulations, and college policy. While the college permits limited personal use of the skidmore.edu email account, faculty and other employees (as well as student employees) do not acquire a right of privacy for communications transmitted on this institutional system. Any of the functions/authority/responsibility assigned to a particular position in this document may be completed by the person holding that position "or his/her designee".

Principles

Custodians of email must not access or disclose the content of email for which they are not correspondents, except in the following situations:

A. In health and safety emergencies; or

B. In response to a court order or other compulsory legal process; or

C. When an email steward (see table 1) has determined that there is a legitimate need to examine email in connection with an investigation involving a human resources matter or a legal or policy violation; or

D. When the information is necessary to conduct time sensitive and or critical college business. Access is tightly controlled and limited, requiring approval of BOTH the respective senior cabinet member and the Director of Human Resources and only after other alternatives have been exhausted.

Reason for the Document

To protect electronic mail from inappropriate access or disclosure and to comply with relevant State and Federal regulations, laws, and policies regarding the protection of certain types of data.

Entities Affected by this Document

All entities of the college.

Who Should Read this Document

All members of the college community

Website Address for this Document

<http://cms.skidmore.edu/it/policies/index.cfm>

Procedures

Requests to Access or Disclose the Content of Email

A. Health and Safety Emergencies

In the event of a health and safety emergency, the college will access and/or disclose the content of email according to the following procedures:

1. IT will access and/or disclose the data upon request by the Director of Campus Safety, Associate Director of Campus Safety, Administrative Director of Health Services, or Member of President's Cabinet.
2. As soon as is practicable, IT will notify the appropriate email steward(s) of the request, what data was accessed and/or disclosed, and any other relevant information, such as the approximate time of the request, access, and disclosure, the name and title of the requester, and the nature of the emergency.
3. As soon as is practicable, IT will notify the Chief Technology Officer.
4. As soon as is practicable, the requesting individual will contact the appropriate email steward (s) (see table 4), informing that individual of the request and the nature of the information received.

B. Court Order or Other Compulsory Legal Process

1. Legal Counsel will review court order to insure validity and authenticity. Legal counsel will provide instruction regarding the college's obligations with said order.

C. Human Resources Matters or Potential Legal or Policy Violations

1. The requesting party must obtain permission from the appropriate email steward(s) of the email (see Table 1, below). If the requesting party is the steward identified in Table 1 (below), permission will need to be granted by the college President.

Table 1

Email Stewards

Member of the college Faculty	Vice President Academic Affairs
Other employees	Director of Human Resources and appropriate cabinet member
Student Employee	Dean of Admissions and Financial Aid or Director of Human Resources
Student	Dean of Student Affairs
President of the College	Chair of the Board of Trustees
Direct Report to the President	President of the College

Note: In an email file, "email correspondents" includes all individuals listed in the "To:" "From:"

“cc:” and “bcc” fields. Therefore, an email may have more than one email steward.

2. The email steward(s) must contact the Chief Technology Officer, providing the details of the request.
3. The Chief Technology Officer will communicate with the appropriate staff member in IT and/or the department requesting access and disclosure of the data to the requester.
4. The IT staff member will confidentially access and disclose the authorized data to the requester.

D. The Information is Necessary to Conduct College Business

I. Forwarding Your Own Email

Faculty or other employees who will be away from their workplaces for any period of time during which access or disclosure of their email may be necessary, should consider forwarding their incoming mail to appropriate parties using a forwarding rule which can be found at: <http://cms.skidmore.edu/it/email/upload/ol2003Forward.pdf>

II. When an Email Account Holder Wishes to Authorize Access by Another Individual to His or Her Account

An email account holder may authorize access to his or her email account on a case-by-case basis.

This provision does not supersede restrictions, such as the prohibition of sharing network passwords. See IT policy Code of Ethics for Computing at Skidmore College:
<http://cms.skidmore.edu/it/policies/ethics.cfm>

This procedure must not be used for human resources matters. For requests involving human resources matters, see **B: Human Resources Matters or Potential Legal or Policy Violations**, above.

III. Rerouting or Forwarding Another Person’s Email

1. The requesting party, generally the party’s supervisor or someone approved by that supervisor, must inform his/her respective cabinet member and upon approval forward to the Director of Human Resources for final approval.
2. The Director of Human Resources will evaluate the request and notify the requesting party of the outcome. If approved, the Director of Human Resources will send the request to the Chief Technology Officer who will work with any applicable department administrator who will effect the rerouting or forwarding.

IV. Accessing a Third Party’s Existing Email

1. The requesting party, generally the party’s supervisor or someone approved by that supervisor, must inform his/her respective cabinet member and upon approval forward to the Director of Human Resources for final approval.
2. The Director of Human Resources will evaluate the request, notifying the requesting party of the outcome. If approved, the Director of Human Resources will send the request to the Chief Technology Officer who will facilitate said access.
3. The requesting party will inform the individual that the request to access their email was made and approved, and the nature of the information received.

Local Support Providers: Ordinary Course of Business

In the course of providing technical support, performing network security and/or maintenance (e.g., backups and restores), local support providers may be required to access, observe, or intercept, but not disclose, reroute, or forward electronic mail messages. There are two circumstances when it is permissible for a local support provider to disclose, reroute, or forward the content of electronic mail messages:

Emergency Exception: Should a local support provider, in the usual course of business, reasonably believe that he or she has accessed information about an emergency involving imminent danger of death or serious injury, the following procedures should be invoked:

1. Contact Campus Safety immediately.
2. As soon as is practicable, report that contact and the underlying information to the Chief Technology Officer, or member of the President's Cabinet. (See "*Reporting Alleged Violations*," below).

Responsible Use Exception: In situations when a local support provider reasonably believes that he or she may have observed evidence of a violation of law or policy, the following procedure should be invoked:

1. As soon as is practicable, reports that contact and the underlying information to the Chief Technology Officer, or member of the President's Cabinet. (See "*Reporting Alleged Violations*," below).

Reporting Alleged Violations

Alleged violations of this policy may be reported to the appropriate individual as detailed in Table 2. Alternatively, you may also contact your supervisor, the college's Chief Technology Officer or a member of the President's Cabinet

Responsibilities

Table 2 outlines the major responsibilities each party has in connection with College Email Policy and Custodianship of Electronic Mail.

Table 2

Director of Campus Safety, Deputy Associate Director of Campus Safety, Director Health Services, Member of President's Cabinet	In health and safety emergencies, contact IT Technical Services with requests to intercept, access, or disclose electronic mail content. In health and safety emergencies, when data has been accessed or disclosed, notify the appropriate email steward of the request and the nature of the information received.
Member of President's Cabinet	Evaluate and approve, or deny requests to have email rerouted or forwarded. Send approved requests to reroute or forward email to the Chief Technology Officer, who will effect the rerouting or forwarding.
Director of Human Resources	Evaluate and approve, or deny, requests to access or disclose electronic mail content in the cases of a human resource matter or potential policy or State and Federal legal violation. Contact the Chief Technology Officer with requests to reroute, forward, intercept, access, or disclose the content of email.
Local Support Provider	Access and disclose specific email messages in cases when information is necessary to conduct college business and the correspondent is unavailable. Access, observe, or intercept the content of electronic mail messages only when performing network security and maintenance functions (e.g., backups and restores). In the usual course of business, disclose, reroute, or forward the content of electronic mail messages only in the following situations: a) In an emergency involving imminent danger of death or serious physical injury; or b) When evidence has been observed of a potential violation of law or policy. In emergencies involving imminent danger of death or serious injury, contact Campus Safety immediately. Report that contact to the Chief Technology Officer or member of the President's Cabinet as soon as possible.

Enterprise Systems, IT	In health and safety emergencies, and upon notification by the appropriate college official, access and disclose requested data. In health and safety emergencies, when data has been accessed or disclosed, notify the appropriate email steward of the request, what data was accessed or disclosed, and any other relevant information, such as the approximate time of the request, access, and disclosure, the name and title of the requester, and the nature of the emergency. In health and safety emergencies, when data has been accessed or disclosed, notify the Chief Technology Officer or Member of President's Cabinet.
Chief Technology Officer	After appropriate permission has been granted by member of President's Cabinet, communicate with appropriate staff to initiate interception, access, or disclosure of electronic mail content. When interception, access, or disclosure of electronic mail content has occurred, inform the individual about whom the request was made of the request, access, and disclosure, where possible and appropriate.
Requesting Individual	In cases of human resources matters or potential legal or policy violations, obtain permission from the appropriate email steward(s) for rerouting, forwarding, intercepting, accessing, or disclosing the content of email. In cases when the information is necessary to conduct college business and the correspondent is unavailable, inform Human Resources, department head, college dean, or Vice President at the time of the request; work with the local support provider to obtain the specific mail messages; and inform the correspondent of the request that was made and of the nature of the information received. In a health or safety emergency, please see "Definitions: Health and Safety Emergency."

Definitions

Definitions apply to terms as they are used in this document.

Table 3

Access	The ability to obtain email content.
Correspondent	Any individual listed in the "To:" "From:" "Cc:" or "Bcc:" fields in the header of an electronic mail message
Custodian	An individual with access to electronic mail data on electronic mail systems.
Disclosure	The act of releasing the content of electronic mail to a third party (e.g., through accessing, intercepting, forwarding, rerouting, etc.)
Email	Electronic mail messages and their associated attachments in a mail user agent (MUA). Note: When data contained in an email message or attachment has been printed or stored outside of the MUA, it is no longer considered email.
Email Steward	The individual, other than a correspondent, with the authority to grant permission for the disclosure of electronic mail content
Health and Safety Emergency	A situation involving an imminent threat of death or serious injury to any person or structure.
Local Support Provider	An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an IT device.
Mail User Agent (MUA)	A program, application, or method used to store, transmit, or receive email.

Contacts

Direct any general questions about College Email Policy Custodianship of Electronic Mail, to your Department Chair or Director. If you have questions about specific issues, call the offices listed in Table 4.

Table 4

Subject	Contact	Telephone	Email/Web Address
Document Clarification and Interpretation	Justin Sipher Chief Technology Officer, Information Technology	(518) 580- 5909	jsipher@skidmore.edu http://cms.skidmore.edu/it/policies/index.cfm
Policy Violations	Barbara Beck Associate Vice President for Finance & Administration and Director of Human Resources	(518) 580- 5809	bbeck@skidmore.edu
	Chief Technology Officer	518) 580- 5909	jsipher@skidmore.edu

Related Documents

Table 5

Documents
Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
Financial Services Modernization Act of 1997
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
USA Patriot Act of 2001
New York Penal Law §240