



LOYOLA UNIVERSITY MARYLAND

**Policy on Custodianship of
Electronic Mail**

November 2010

Table of Contents

I. Purpose.....	1
II. Scope.....	1
III. Definitions.....	2
IV. Policy	2
V. Responsibilities	3
VI. Procedures.....	5
VII. Penalties and Enforcement.....	8
VIII. Annual Reporting.....	8
IX. Approvals	8



LOYOLA UNIVERSITY MARYLAND

Policy on Custodianship of Electronic Mail

Loyola University Maryland (the “University”) owns and operates its electronic mail (e-mail) infrastructure, which must be managed for the entire University community in a manner that preserves a level of privacy and confidentiality in accordance with applicable regulations, laws, and University policy. While the University permits limited personal use of its e-mail infrastructure, those availing themselves of this privilege do not acquire a right of privacy in communications transmitted or stored on University information technology resources. Personal e-mail is subject to review when there is reasonable cause to do so, as set forth in this policy. Personal use must also comport with the University’s policies, code of conduct, and ethics.

The University strives to protect e-mail from inappropriate access or disclosure in order to contribute to the trust of University information technology systems and to comply with applicable regulations, laws and policies regarding the protection of certain types of data.

I. Purpose

The purpose of this Custodianship of Electronic Mail Policy (the “Policy”) is to define security practices that will allow the University to:

- Comply with applicable regulations, laws, and policies regarding the protection of certain types of electronic data.
- Identify situations when the University may allow and provide access to an e-mail account without the permission of the account holder.

II. Scope

This Policy applies to all entities and persons using the University’s e-mail system including, but not limited to, all faculty, staff, administrators, students, alumni, consultants, and any person or agency employed or contracted by the University or any of its auxiliary organizations.

III. Definitions

In this Policy, certain terms are defined as follows:

TERM	DEFINITION
Access	The ability to obtain e-mail content.
Correspondent	Any individual listed in the "To:," "From:," "Cc:," or "Bcc:" fields in the header of an electronic 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.).
E-mail	Electronic mail messages and their associated attachments and content in a mail user agent (MUA). Note: When data contained in an e-mail message or attachment has been printed or stored outside of the MUA, it is no longer considered e-mail.
E-mail Steward	An individual, other than a correspondent, with the authority to grant permission for the access or disclosure of e-mail for legitimate University purposes, e.g., in connection with an investigation involving a potential legal or policy violation or a human resources matter.
Health and Safety Emergency	A situation involving an imminent threat of death or serious injury to any person.
Local Support Provider	An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device (e.g., system administrator or network administrator).
Mail User Agent (MUA)	A program, application, or method used to store, transmit, or receive e-mail.
Requesting Individual	An individual seeking access or disclosure of e-mail.

IV. Policy

Custodians of e-mail must not access or disclose the content of e-mail in which they are not correspondents, except in the following situations:

- A) In response to a court order or other compulsory legal process, including a subpoena or discovery request; or
- B) When an E-mail Steward has determined that there is a need to examine e-mail for legitimate University purposes, e.g., in connection with an investigation involving a potential legal or policy violation or a human resources matter; or
- C) For faculty, administrators, staff, student employees, temporary employees and contractors (who have a Loyola e-mail account), when the information contained within the e-mail is necessary to conduct University business, all reasonable efforts have been made to contact the account holder and the account holder is unavailable for an unacceptable period of time; or
- D) In health or safety emergencies.

V. Responsibilities

The following chart describes the major responsibilities each party or office has in connection with the Policy:

Director of Public Safety and Campus Police, Assistant Director of Campus Police, Director of the Student Health Center, Assistant Vice President for Human Resources	<p>In health and safety emergencies, direct the Office of Technology Services to access or disclose e-mail.</p> <p>When data has been accessed or disclosed in a health and safety emergency, notify the appropriate E-mail Steward (as set forth in subsection VI(B)) and the Chief Information Officer or Director of Technology Support of the request and the nature of the information accessed or disclosed.</p>
E-mail Steward (Vice President for Academic Affairs, Vice President for Administration, or Vice President for Student Development)	<p>Approve or deny requests to access or disclose e-mail pursuant to subsections VI(B), (C), and (D) of this Policy.</p> <p>Determine whether it is appropriate to inform correspondents that their e-mail has been accessed or disclosed.</p> <p>Contact the Chief Information Officer or Director of Technology Support with approved requests to access or disclose e-mail and whether the affected e-mail correspondents should be informed of the access or disclosure.</p>
Vice President for Administration	<p>Accept service of court orders or other compulsory legal process, including subpoenas and discovery requests. Approve access or disclosure of e-mail in response to such legal papers where the legal papers are valid and the request for access or disclosure is proper (after consultation with the University's attorneys if necessary).</p>
Chief Information Officer, or Director of Technology Support	<p>Communicate with appropriate staff to effectuate approved requests to access or disclose e-mail.</p> <p>If ordered by an E-mail Steward, inform correspondents that the correspondents' e-mail has been accessed or disclosed.</p>
Office of Technology Support (OTS)	<p>Access and disclose e-mail pursuant to subsections VI(A), (B), (C), and (D) when access or disclosure has been approved as required under this Policy.</p> <p>When e-mail has been accessed or disclosed in a health and safety emergency, notify the appropriate E-mail Steward and the Chief Information Officer or Director of Technology</p>

Support 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.

OTS may also access or disclose e-mail:

a) when performing network security and maintenance functions (e.g., backups and restores).

b) in an emergency involving imminent danger of death or serious physical injury*; or

c) when evidence has been observed of a potential violation of law or policy.

*In emergencies involving imminent danger of death or serious injury, contact Public Safety (x5911) and 911 immediately. As soon as possible thereafter, notify the appropriate E-mail Steward and the Chief Information Officer or Director of Technology Support of the circumstances of the access or disclosure.

Assistant Vice President for Human Resources, Unit Human Resources Representative, Unit Head, College Dean, Vice President, or E-mail Steward

Approve or deny requests to access or disclose existing e-mail when the correspondent is unavailable and the information is necessary to conduct University business.

Assistant Vice President for Human Resources

Approve or deny requests to have another correspondent's e-mail rerouted or forwarded when the information is necessary to conduct University business and the correspondent is unavailable.

Requesting Individual

In response to a court order or other compulsory legal process, notify the Vice President for University Administration.

In cases of human resources matters or potential legal or policy violations, obtain permission from the appropriate E-mail Steward(s) for accessing or disclosing e-mail.

In cases when the information is necessary to conduct University business and the correspondent is unavailable:

1) obtain permission from the Assistant Vice President for Human Resources to have another correspondent's e-mail rerouted or forwarded; and

2) obtain permission from the Assistant Vice President for Human Resources, a unit human resources representative, unit head, college dean, or vice president to access or disclose another correspondent's existing e-mail.

Contact the Office of Technology Support with approved requests to access or disclose e-mail. Inform the correspondent of the request that was made and of the nature of the information received.

In a health or safety emergency, notify the Director of Public Safety and Campus Police, Assistant Director of Campus Police, Director of the Student Health Center, Assistant Vice President for Human Resources, or an E-mail Steward.

VI. Procedures

A) Court Order or Other Compulsory Legal Process

University employees who are contacted by an individual attempting to serve legal papers, including a court order or other compulsory legal process, such as subpoenas or discovery requests, should direct the individual attempting to serve such legal papers to the Vice President for University Administration. The Office of the Vice President for University Administration will accept service of legal papers. Legal papers received through the mail should also be directed to the Office of the Vice President for University Administration. The Vice President for University Administration will permit access or disclosure of e-mail when the legal papers are valid and the request for access or disclosure is proper. If necessary, the Vice President for University Administration will confer with the University's attorneys regarding whether to permit access or disclosure.

B) Human Resources Matters or Potential Legal or Policy Violations

1. The requesting party must obtain permission from the appropriate E-mail Steward(s) or from a designee as set forth in the table below:

E-MAIL CORRESPONDENT	E-MAIL STEWARD(S)
Members of the University Faculty	Vice President for Academic Affairs
Members of the Administration, Staff or Alumni	Vice President for Administration
Students, prospective Students and Student Employees	Vice President for Student Development
All Others	Vice President for Administration

Note: Because "correspondent" includes all individuals listed in the "To:," "From:," "Cc:," or "Bcc:" fields, an e-mail may have more than one E-mail Steward.

2. The E-mail Steward must contact the Chief Information Officer or Director of Technology Support to provide details of an approved request.
3. The Chief Information Officer or Director of Technology Support will direct appropriate staff to access and disclose the e-mail to the requester.

Note: In cases of potential legal violations, the E-mail Steward should contact the University's attorneys when appropriate. In cases of potential violations of University policy, the E-mail Steward should contact the University Compliance Officer when appropriate.

C) Information Necessary to Conduct University Business (other than Human Resources Matters or Potential Legal or Policy Violations)

1. Forwarding Your Own E-mail:

Faculty or staff members who will be away from their workplaces for any period of time during which access or disclosure of their e-mail may be necessary should consider forwarding their incoming mail to appropriate parties.

2. Rerouting or Forwarding Another Person's E-mail

- a. The requesting party, generally the supervisor, must inform the unit human resources representative of the request to have e-mail rerouted or forwarded to another specific e-mail account.
- b. The unit human resources representative will send the request to the Assistant Vice President for Human Resources.
- c. The Assistant Vice President for Human Resources will approve or deny the request and notify the requesting party of the outcome. If the request is approved, the Assistant Vice President for Human Resources will send the request to the University's Chief Information Officer or Director of Technology Support who will direct appropriate staff to reroute or forward the e-mail to the requester.

3. Accessing a Third Party's Existing E-mail

- a. The requesting party, generally the correspondent's supervisor, must inform one of the following individuals of the request to access or disclose another correspondent's existing e-mail due to the account holder's being unavailable for an unacceptable period of time: Assistant Vice President for Human Resources, the unit human resources representative, unit head, department chair, college dean, vice president (including an E-mail Steward), who will approve or deny the request and notify the requesting party of the outcome.
- b. If the request is approved, the requesting party may then contact the Office of Technology Support to obtain the specific e-mail messages.

- c. The requesting party will inform the correspondent in writing, within a reasonable period of time that the request was made and approved, including the audit trail and of the nature of the information received.
4. When an E-mail Account Holder Wishes to Authorize Access by Another Individual to His or Her Account
 - a. An e-mail account holder may authorize access to his or her e-mail account on a case-by-case basis.
 - b. This provision does not supersede restrictions contained in any other University policies, such as the prohibition of sharing e-mail account passwords.
 - c. The e-mail account holder remains responsible for the security of the e-mail account and the information contained therein. The e-mail account holder may be subject to disciplinary action for any adverse consequences resulting from the e-mail account holder's decision to authorize access by another individual to the e-mail account.

D) Health and Safety Emergencies

In the event of a health or safety emergency, the University will access or disclose the content of e-mail according to the following procedures:

1. Upon request by the Director of Public Safety and Campus Police, Assistant Director of Public Safety, Director of the Student Health Center, Assistant Vice President for Human Resources, or an E-mail Steward, the Office of Technology Support will access and disclose the requested e-mail content.
2. As soon as is practicable, the Office of Technology Services will notify the appropriate E-mail Steward (as set forth above in VI(B)(1)), the Chief Information Officer, and the Director of Technology Support of the request, of what data was accessed and disclosed, and of 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.

E) Permitted Access and Disclosure by the Office of Technology Support

In the course of performing network security and maintenance functions (e. g. backups and restores), the Office of Technology Support (OTS) may be required to access, observe, or intercept, but not disclose, reroute, or forward e-mail messages. There are two additional circumstances when it is permissible for OTS to disclose, reroute, or forward the content of e-mail messages:

1. Emergency Exception: If OTS, in the usual course of business, reasonably believes it has accessed information about an emergency involving imminent danger of death or serious injury, it should:

- a. Immediately contact Public Safety (x5911) and call 911; and
 - b. As soon as possible, thereafter, report the information to the Chief Information Officer or Director of Technology Support.
2. Responsible Use Exception: When an individual in OTS has reasonable cause to believe there may be a violation of law or policy occurring, University policy requires the individual to report this information to the Technology Services Information Security Office. For more information, refer to the University's Information Security Policy (<https://www.loyola.edu/CIO/Documents/InfoSecurityPolicy.pdf>). Reports may also be filed with EthicsPoint.com through the link on the human resources page.

VII. Penalties and Enforcement

Violators of this policy are subject to disciplinary action as specified in the Staff and Administrators Policy Handbook and the Student Community Standards Handbook.

VIII. Annual Reporting

The Office of Technology Services will prepare an annual report, appropriately redacted, listing the frequency of use taken under each action, relative to this policy. This report will be submitted to the Loyola Conference at the end of the academic year and posted on the Technology Services Policy website; <http://www.loyola.edu/CIO/Policies/>.

IX. Approvals

Preparer Name and Title: Louise Finn, Chief Information Officer

Preparer Signature: Louise Finn

Date: 12-3-10

Reviewed and approved by the President's Cabinet and the Loyola Conference

Final Approval Name and Title: Brian Linnane, S.J. President

Final Approval Signature: Brian Linnane

Date: 12-3-10