Electronic Mail and Voice Mail Use and Disclosure

Policy Title:
Electronic Mail and Voice Mail Use and Disclosure

Responsible Executive(s):
James Pardonek, Director and Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This document sets forth Loyola University Chicago's policy regarding access and disclosure of electronic mail or voice mail messages sent or received by university faculty, students, and staff through Loyola's email and voicemail systems. It also sets forth policies on the proper use of these systems. While other Loyola policies do address the issues of information privacy and use of university resources (see Related Policies at Loyola in this document), there are aspects of email and voicemail which these policies do not address that are addressed in this document.

II. Definitions

Not applicable.

III. Policy

Permissible Uses of Email and Voice Mail

Loyola provides email and voicemail to its faculty, students, and staff for educational, research, and other business purposes. Members of the Loyola community should limit their use to these purposes.

Persons outside the Loyola community may be given access to Loyola email and voicemail on a case-by-case basis by special authorization from Information Technologies and under certain conditions, including adherence to this and other applicable policies.

The use of electronic mail and voice mail at Loyola should comply with other University policies regarding computing facilities and disclosure of information. This includes Loyola policies on the authorized use of public computing facilities, ethical conduct for computer use, and handling of confidential information.

Official Business Email Usage

Loyola University Chicago mandates that all official business emails will be sent exclusively from/to your official university email address. It is the responsibility of all employees to regularly check their university email and respond promptly to any necessary communications. Faculty

members are required to use their university email address for all correspondence with students and to include this email address in their syllabi.

Confidentiality of Electronic Mail

Loyola cannot guarantee the confidentiality or privacy of email or voicemail messages and makes no promises regarding their security. Decisions as to what information to include in such messages should be made in accordance with the Data Classification Policy.

The following elements guide the administration of email and voicemail at Loyola as it relates to confidentiality:

- **Administrative Activities:** Loyola reserves the right to conduct routine maintenance, track problems, and maintain the integrity of its systems. As is the case with all data kept on Loyola's computer systems, the contents of electronic or voice mail messages may be revealed by such activities.
- **Monitoring:** Loyola does not monitor the contents of electronic or voice mail messages as a routine matter. However, such monitoring may be conducted when required to protect the integrity of the systems or to comply with legal obligations.
- **Directed Access:** Loyola reserves the right to inspect the contents of email and voicemail messages during an investigation triggered by indications of impropriety, during a legal investigation, or as necessary to locate substantive information that is not more readily available by some other less intrusive means. Loyola will comply with all legal requirements for access to such information.

Limitation on Disclosure

Any third-party disclosure of the contents of electronic or voice mail obtained according to this policy will be limited unless such disclosure is required to protect the integrity of Loyola's systems or to comply with a legal obligation.

Violations

The University's standard conduct procedures for violations will apply, as outlined in the following documents:

- Student Handbook – for students
- Faculty Handbook – for faculty
- Employee Handbook and Personnel Policies – for staff

Violations of policies governing the use of email, computing, networking, telephony, and information systems may result in suspension or revocation of access privileges by system administrators. Additionally, such violations may lead to disciplinary action under the applicable University conduct standards. Where appropriate, incidents may also be referred for civil or criminal investigation in accordance with local, state, or federal laws.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Jim Pardonek, Director and Chief Information Security Officer	Enforcing the Policy at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- Acceptable Use Policy
- Security Policy
- Faculty Handbook
- Student Handbook
- Employee Handbook
- Ownership and Use of Data

Approval Authority:	IT Steering Committee	**Approval Date:**	April 1, 2006
Review Authority:	Jim Pardonek	**Review Date:**	June 16, 2025
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu