Electronic Mail and Voice Mail Use and Disclosure Policy

Policy Title:
Electronic Mail and Voice Mail Use and Disclosure Policy

Responsible Executive(s):
Jim 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 electronic and voice mail 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 electronic and voice mail which these policies do not address that are addressed in this document.

II. Definitions

Not applicable.

III. Policy

Permissible Uses of Electronic Mail and Voice Mail

Loyola provides electronic and voice mail to its faculty, students, and staff for educational, research, health care, and internal 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 electronic and voice mail 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. In particular, this includes Loyola policies on the authorized use of public computing facilities, ethical conduct for computer use, and handling of confidential information.

Confidentiality of Electronic Mail

Loyola cannot guarantee the confidentiality or privacy of electronic or voice mail 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 electronic and voice mail 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 electronic and voice mail messages in the course of an investigation triggered by indications of impropriety 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 use of electronic mail services is a privilege offered to Loyola faculty, staff, and students. Loyola University Chicago reserves the right to revoke this privilege for violations of this policy.

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:

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

Approval Authority:	ITESC	**Approval Date:**	April 1, 2006
Review Authority:	Jim Pardonek	**Review Date:**	July 16, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu