Use of Electronic Mail Systems Policy

Policy Title:
Use of Electronic Mail Systems 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

Electronic mail (e-mail) has become a ubiquitous service greatly enhancing communication both internally within the Purdue community and externally to Users, including prospective students, alumni, and the public at large. The purpose of this policy is to describe the appropriate use of University E-mail Facilities, associated responsibilities, and rights of all Users of University E-mail Facilities and Official University E-mail Accounts.

II. Definitions

Not applicable.

III. Policy

Loyola University Chicago provides computing, networking, telephony and information resources for access and use by students, faculty, staff and other persons associated with the University. These resources include the access and use of the university electronic mail systems. The University community is encouraged to use electronic mail to enhance productivity through the efficient and cost-effective exchange of information to advance the education, research, and public service missions of the University.

The University has the responsibility and duty to maintain the integrity, operation and availability of its electronic mail systems for access and use by the University community. Access to the University network and its electronic mail systems is a privilege and certain responsibilities accompany that privilege. All electronic mail files which are transmitted and received using University networks or which are stored on University systems are University records.

This policy pertains to the access and responsible use of University electronic mail systems. All who access and use University electronic mail systems must abide by all applicable policies, legal and contractual requirements, and the highest standard of ethical principles and practices, when using this university resource.

Use of University electronic mail systems will constitute awareness and acceptance of the responsibilities regarding the access and responsible and ethical use of these systems as presented in this and other access and acceptable use policies of University computing, networking, telephony and information resources.

Individuals covered

This policy applies to all students, faculty, staff, and any other person extended access and use privileges by the University.

Electronic mail systems covered

This policy applies to all electronic mail systems operated or contracted by the University, or connected to the University network. The policy also applies to any electronic mail transmission identified (e.g., the From: field in the mail header) with an electronic mail address containing the Internet domain name assigned to the University, i.e., luc.edu.

Guidelines on electronic mail use

Access to and the responsible and ethical use of information technology are essential to the pursuit and achievement of excellence at Loyola University Chicago. The University encourages appropriate use of its electronic mail systems to enhance productivity through the efficient and cost-effective exchange of information to advance the University's mission in education, research and public service. Use of these resources must be consistent with these goals. These resources must not be used to impede or hinder the University mission. The primary use of a University electronic mail system must be related to the University's educational, research and public service missions and to the person's educational, scholarly, research, service, operational or management activities within the University. Incidental and occasional personal use is permitted, but it is expected to comply with all university policies and it will be treated no differently than other e-mail messages. As responsible and ethical members of the University community, we are expected to act by the following general guidelines based on common sense, common decency, and civility applied to the University networked computing environment.

- Respect the rights and personhood of others. Do not send electronic mail, messages, postings or materials that serve to abuse, insult, intimidate, threaten or harass others; to interfere unreasonably with a person's work or educational performance; or to create an intimidating, hostile or offensive learning/working environment, especially within the context of other University policies, i.e., Policy and Procedures on Sexual Harassment and Policy and Procedures for Racial Discrimination, Abuse and Harassment. Civil discourse is at the heart of a University free from intimidation and harassment and based upon a respect for individuals and a desire to learn from others. While debate on controversial issues is inevitable and essential, bear in mind that it is your responsibility to do so in a way that actually advances the cause of learning and mutual understanding.
- Messages sent as electronic mail should meet the same standards for distribution or display as if they were tangible documents or instruments. Identify yourself clearly and accurately in all electronic communications. Concealing or misrepresenting your name or affiliation to dissociate yourself from responsibility for your actions is never appropriate. Alteration of the source of electronic mail, message or posting is unethical and may be illegal.
- Do not access e-mail files stored in someone else's mailbox unless you have authorization or proxy rights of access.
- Be sensitive to the inherent limitations of shared network resources. No computer security system can absolutely prevent a determined person from accessing stored information that they are not authorized to access. While the University has no interest in regulating the content of electronic mail, it cannot guarantee the privacy and confidentiality of electronic documents. Good judgment dictates the creation of electronic documents that may become available to the public.
- Furthermore, be aware that electronic mail sent to recipients at public educational institutions and public agencies may be subject to disclosure under governmental open records laws.

- Promote the efficient use of University computing and networking resources consistent with the University's mission in education, research and public service. Show consideration for others and refrain from engaging in any use that would interfere with their work or disrupt the intended use of computing and networking resources. Refrain from wasteful and disruptive practices, such as sending "chain letters," "spamming" messages, unsolicited junk mail, "broadcast" messages about non-University business, or unwanted material, either locally or on the Internet at large.
- Conserve University electronic mail system resources. Be responsible for the content and maintenance of your electronic mailbox on any University electronic mail system. Check your E-mail frequently. Delete unwanted messages immediately since they consume disk storage. Keep messages remaining in your electronic mailbox to a minimum. If possible, archive your messages or download them from your electronic mailbox to your personal computer's hard drive or to diskettes. Do not use electronic mail and other network resources for commercial purposes or personal financial gain, without permission from the University.
- Do not use electronic mail and other network resources to send or distribute copies of documents and files (including audio, video and graphics) in violation of copyright laws.
- Be prudent in the use of electronic discussion lists. Limit your use as much as possible. Many electronic discussion lists are available in other forms, e.g., Usenet News and the World Wide Web. Using these other means of accessing these lists will require fewer computing and networking resources than subscribing to a list. If you do subscribe to an electronic discussion list, always make sure that you know how to unsubscribe from that list, and do so when you no longer have a use for the information from the list, or when you are ready to stop using the electronic mail system at the University. Be careful when sending to electronic discussion lists. Sending large messages to lists that may have hundreds of subscribers can dramatically affect the electronic mail system from which you are sending the message and the electronic mail systems receiving the message. Before sending to any electronic discussion list or replying to any message from an electronic discussion list, make sure to know the guidelines and policies of that list. Be aware of where the message is going (to the entire list or just to the person that sent the original message).
- Refrain from forwarding electronic mail messages without a legitimate business purpose under circumstances likely to lead to embarrassment of the sender or to

violate clearly expressed desire of the sender to restrict additional dissemination.

The same standards of conduct expected of students, faculty and staff regarding the use of telephones, libraries and other institutional resources apply to the use of electronic mail systems. You will be held no less accountable for your actions in situations involving electronic mail than you would be in dealing with other communications media. You are expected to abide by the security restrictions on all systems and information to which you have access. You should avoid any communication where the meaning of the message, or its transmission or distribution, would be illegal, unethical or irresponsible. Conduct that involves the use of electronic mail to violate a University policy or regulation, or to violate the rights of another, is a serious abuse subject to limitation of your electronic mail and networking access privileges and appropriate disciplinary action.

Privacy on University electronic mail systems

The University community must recognize that electronic communications are hardly secure and the University cannot guarantee privacy. The University will not monitor electronic mail messages as a routine matter. But the University reserves the right to inspect, access, view, read and/or disclose an individual's computer files and e-mail that may be stored or archived on University computing networks or systems, for purposes it deems appropriate. There may arise situations in which an individual's computer files and e-mail may be inspected, accessed, viewed, read and/or the contents may be revealed or disclosed. These situations include but are not limited to:

- During ordinary management and maintenance of computing and networking services,
- During an investigation of indications of illegal activity or misuse, system and network administrators may view an individual's computer files including electronic mail,
- During the course of carrying out the University's work, to locate substantive information required for University business, e.g., supervisors may be need to view an employee's computer files including electronic mail,
- If an individual is suspected of violations of the responsibilities as stated in this document or other University policies,
- To protect and maintain the University computing network's integrity and the rights of others authorized to access the University network.

- The University may review and disclose contents of electronic mail messages in its discretion in cooperating with investigations by outside parties, or in response to legal process, e.g., subpoenas,
- Should the security of a computer or network system be threatened.

Integrity and confidentiality on university electronic mail systems

Just as the University cannot guarantee privacy when it comes to electronic mail systems, the University cannot guarantee the integrity of all electronic mail messages, e.g., content and mail headers of electronic mail messages can be modified before they are forwarded to another recipient. The University also cannot guarantee the preservation of confidentiality of any information passing through its electronic mail systems. The University electronic mail systems should not be used to transmit sensitive or confidential information without the use of more secured methods, e.g., encryption devices. In general, if the information should not be appearing in a local newspaper it should not be sent through the University electronic mail system without the use of more secured methods. Use discretion and keep in mind that an electronic mail message transmitted without the use of more secured methods is similar to a post card.

Actions of system administrators of University electronic mail systems

A system administrator of a University electronic mail system may determine within his or her discretion when it is necessary to temporarily suspend access to the electronic mail system to insure the integrity and operation of the electronic mail system and its availability to the University community. System administrators who suspend access of students to University electronic mail systems should report the actions to the Office of Student Affairs as soon as possible, along with an explanation for taking the action. In some cases, system administrators may need to work with the Office of Student Affairs to make arrangements to permit these students sufficient access to the University electronic mail to complete course work.

Appeal of an administrative decision

Individuals who disagree with a decision of a system administrator of a University electronic mail system may submit an appeal of the decision to the appropriate resource manager or systems administrator. From there, a student may submit an appeal to the Dean of Students, a faculty member through their department administration either to the Senior Vice President Dean of Faculties or to the Senior Vice President for the Health Sciences, and a staff member through their management to the Vice President for

Human Resources. Individuals must submit these appeals according to any rules and procedures issued by system or network administrators, or component administrators.

Noncompliance and sanctions

Reports of incidents regarding inappropriate use of University electronic mail systems as they pertain to this policy should be referred to the Dean of Students if the alleged sender is a student, to the academic department or institute administrator, if the alleged sender is a faculty member, and to the immediate supervisor if the alleged sender is a non-faculty staff member. Breach of or disregard for this and other policies and procedures concerning access and acceptable use of computing, networking, telephony and information resources may result in the denial or removal of access privileges by system or network administrators, and may lead to disciplinary action under the applicable University's standards of conduct, i.e., Student Handbook (students), Faculty Handbook (faculty) and Employee Handbook and Personnel Policies (staff). Additionally, such disregard may be referred to other authorities for civil litigation and criminal prosecution under applicable state and federal statutes. As e-mail is a privilege extended to the University community to facilitate communication, staff members should utilize it ethically and within bounds of this and other University policies. Staff employees can be disciplined for misuse or unauthorized use of e-mail up to and including suspension of privileges for a particular period of time, suspension from the job or termination. Such actions can be taken by the department head in consultation with Human Resources as part of the Progressive Discipline procedure. In some cases, the University authority handling the incident report may request that the system administrator suspend the access to a University electronic communication system by the individual under investigation. For example, the Office of the Dean of Students may request that access be suspended pending the outcome of conduct hearing process, or a department administrator may request that access be suspended for a staff person pending the outcome of an investigation or disciplinary process.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Jim Pardonek, Associate 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

Approval Authority:	ITESC	**Approval Date:**	September 11th, 2013
Review Authority:	Jim Pardonek	**Review Date:**	March 7th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu