


<b>Name of Policy:</b> <a href="#">Electronic mail services policy.</a> <b>Policy Number:</b> 3364-65-01 <b>Approving Officer:</b> President <b>Responsible Agent:</b> Vice President of Information Technology <b>Scope:</b> All University of Toledo Campuses		 <b>Original Effective date:</b> January 29, 2009
	<input type="checkbox"/> New policy proposal <input checked="" type="checkbox"/> Major revision of existing policy	

(A) Policy statement

The University of Toledo provides electronic mail to support academic, research, medical, and administrative functions of the institution. University E-mail services are to be used responsibly within the normal standards of professional and personal courtesy and conduct. The use of E-mail services is a privilege, not a right, and it should be treated as such by all users.

(B) Purpose

This policy establishes guidelines for the responsible and efficient use of The University of Toledo (university) electronic mail, hereinafter "E-mail," services and to clearly set forth the rights and responsibilities of university authorized users regarding their use of E-mail.

(C) Scope of policy

E-mail communications and associated attachments transmitted or received over the university network are subject to the provisions of this policy. According to Ohio law E-mail communications are generally considered to be public records. E-mail communications written and sent in the course of University business are subject to applicable provisions of this policy, regardless of whether the communication was sent or received on a public or privately owned personal computer.

(D) Application of Ohio Public Records Law to E-Mail

(1) E-mail messages are subject to the same legal requirements as most other forms of communication. The Ohio Public Records Act, Ohio Revised Code §149.43 governs availability of public records. The Ohio Public Records Act treats electronic records in the same manner as paper records.

(2) E-mail messages that document the functions, policies, and procedures of the University are public records that must be retained in either paper or electronic format. Disposition decisions regarding individual documents should be made

with cognizance of the definition of public records and in accordance with university Record Retention policy.

(E) General principles and rules

(1) Authorized users.

Authorized users of the campus electronic mail system may include the following based upon need and available resources:

- (a) Employees of the university.
- (b) Students designated as active per the registrar's office.
- (c) Other users as approved by the vice president for information technology or designee.

(2) Management.

- (a) Employees and other authorized users who elect to leave the university will have their mailboxes deleted after documents needed by their department are identified and archived. Those employees who have been terminated or who have received notification of termination will be immediately restricted from access to the system, unless expressly permitted by the appropriate vice president or designee.
- (b) Students not currently enrolled at the university will be restricted from access to the system and their mailboxes may be deleted.

(3) Authorized access and disclosure

Access to university email, when provided, is a privilege that may be wholly or partially restricted by the university without prior notice and without the consent of the user. The university reserves the right to monitor, inspect, and disclose usage without prior notice.

Dependent upon the circumstances, E-mail privileges may be suspended or revoked as well as invoking appropriate sanctions and reprimand depending upon the severity and circumstances of the situation.

The university information security office may institute scanning and/or blocking technologies based on these prohibitions, or other material issues, for the protection of the university and university owned information technology assets.

(4) Privacy and confidentiality

Confidentiality and privacy of E-mail messages cannot be guaranteed because many E-mail communications are public records. Authorized users should review the content and attachments of E-mails to ensure that the message would not be a source of embarrassment to the sender, to the recipient, or to the university.

Authorized users should exercise extreme caution when using email services to communicate confidential or sensitive matters. Users should employ protections such as; password protecting files, encrypting messages, etc. Users that are unsure how to protect content should contact the information technology help desk.

(F) Responsible use

(1) In order to ensure responsible use of E-mail, authorized users using E-mail to transmit data should ensure:

- (a) Recipients of the E-mail are intended users of the information transmitted;
- (b) Virus checking is performed on all attachments before opening them on the university network;
- (c) A disclaimer is attached to applicable outgoing email. A couple of examples are below:

- (i) “This email and any files transmitted are confidential. They are intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient, be advised that you have received this email in error, and that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited.”

- (ii) “ This message and any response to it may constitute a public record and therefore may be available upon request in accordance with Ohio public records law.”

(2) Computer equipment

Unattended computers could be used by unauthorized users. It is the responsibility of the user to ensure that when leaving a computer unattended appropriate safeguards are in place to ensure security.

(G) Protected information

Protected information includes protected health information (PHI), personally identifiable information (PII), and payment card information (PCI.) (See definitions of PHI, PII, and PCI) In the event that protected information or other confidential information is sent in an email message, it should be protected appropriately and sent to only those individuals with a need to know. Protected information shall not be transmitted to any external, email addresses unless it has been encrypted. If required, authorized users can contact the information technology help desk for assistance.

(H) Personal use by employees

University equipment and E-mail service may be used by employees for incidental personal purposes as long as the personal use does not interfere:

- (1) with the performance of his or her job responsibilities;
- (2) with the business use of E-mail by other authorized users;
- (3) does not burden the university with noticeable incremental cost(s);
- (4) with the user's employment or other obligations to the university.

(I) Institutional communication

Communication by E-mail to the entire address book or large portions of the address book must be approved and distributed by the office of marketing and communications. The office of marketing and communications will work with the departments to select and utilize the most appropriate means to disseminate information to the entire university community.

(1) Exceptions

Some communications, such as electronic infrastructure outages, health, security, and safety issues and messages from the president may go out directly as necessary.

(J) Retention

University records in electronic form including documents, email, and backup copies should be retained in accordance with the university's record retention schedules that apply to non-electronic records of similar subject and content. If necessary, specific departmental retention schedules for unique records in electronic form can be established. The university archivist is responsible for establishing records retention schedules.

(K) Prohibited uses and procedures

The following is a list of practices that are prohibited on university provided E-mail systems. This is not an all inclusive list; the university may revise this list as necessary.

- (1) Harassment, intimidation, or threatening another person.
- (2) Accessing or distributing obscene, sexually explicit, or abusive materials, including but not limited to racial slurs, gender-specific comments or any comment/material that would offend someone on the basis of his or her age, sexual orientation, religious or political beliefs, national origin, or disability.
- (3) Illegally distributing copyrighted materials.
- (4) Initiating or forwarding chain mail.
- (5) Pursuing personal business interests not related to the university.
- (6) Any purpose that is illegal, against policy, or against the university mission.
- (7) Deliberately sending large volumes of mail or attachments to purposely waste resources.
- (8) Selling or soliciting the purchase of personal items.
- (9) Obtaining access to email of others for the purpose of satisfying idle curiosity, with no substantial university purpose.
- (10) Attempt unauthorized access to email or attempt to breach any security measures on any email system, or attempt to intercept any email transmissions without proper authorization.
- (11) Employing false identities or unauthorized sending of email on behalf of others.

(L) Definitions

- (1) E-Mail means an electronic message transmitted between two or more computers or electronic terminals, whether or not the message is converted to hard copy format after receipt and whether or not the message is viewed upon transmission or stored for later retrieval.
- (2) Payment Card Information (PCI): PCI is information associated with payment cards such as card numbers and associated personal identification numbers.
- (3) Personally Identifiable Information (PII): PII is information that can be used to distinguish or trace your identity. Primary examples of PII are social security numbers or information that, when combined or used with other identifying information, is linked or linkable to a specific individual. Social security numbers are explicitly defined as PII and shall be protected.
- (4) Protected Health Information (PHI): PHI is information that could reasonably lead to the identification of an individual, either by itself or in

combination with other reasonably available information.

Legal counsel should be consulted if there is uncertainty about whether or not a particular public office is a “covered entity” for purposes of HIPAA.

- (5) Public Records means all writings made, maintained, or kept by the state, or any agency, institution, or subdivision thereof, for use in the exercise of functions required or authorized by law or administrative rule, or involving the receipt or expenditure of public funds.
- (6) The Privacy Rule protects all “individually identifiable health information,” which is called “protected health information,” or “PHI.” The HIPAA regulations, including the Privacy Rule, apply only to covered entities.
- (a) Health Care Components: are covered entities of the university for purposes of HIPAA compliance. The privacy officer maintains the lists of university health care components.

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>January 29, 2009</u> Date</p> <p><i>Review/Revision Completed by: Vice President of Information Technology</i></p>	<p><b>Policies Superseded by This Policy:</b></p> <ul style="list-style-type: none"> <li>• <i>01-070 Electronic Mail Services Policy (former Health Science Campus policy last reviewed 07/01/03)</i></li> <li>• <i>3360-70-03 E-mail use (Main Campus policy last reviewed 08/30.02)</i></li> <li>• <b>Initial Effective Date:</b> January 29, 2009</li> <li>• <b>Review/Revision Date:</b></li> <li>• <b>Next review date:</b> January 29, 2012</li> </ul>
--	--