

OSU INSTITUTE OF TECHNOLOGY
POLICY & PROCEDURES

<p>Use of Email</p>	<p>6-002 TECHNOLOGY SERVICES December 2019</p>
---------------------	---

POLICY

- 1.01 With the availability of expanding access to electronic communications, including electronic mail (email), comes the need for university policy to inform members of the university community (all those individuals who are using email on university-issued accounts) on issues of appropriate use, privacy, and access of email. This document is an attempt to provide policy that will assist the university community to understand and exercise the use of this technology in pursuit of the goals of the university. The policy statements refer only to email. It is recognized that the law governing electronic communication technologies and the material transmitted using these technologies is in an early stage of development and that the policy statements in this document will change in response to changes in law and further development of electronic communications technology.

This policy will apply to all university email services. Members of the university community who are given access to OSU Institute of Technology's (OSUIT) email system will be informed of the policies in this document and will be required to agree to applicable policies. Violations of this policy will result in loss of email privileges at the university, disciplinary action, or legal action where applicable.

PROCEDURES

Appropriate Use

- 2.01 As with other university resources, email is appropriately used for purposes that further the goals of the university.
- 2.02 Individuals may not use email for entrepreneurial activities except in cases of university-sanctioned activities.
- 2.03 No one shall be added to an email mailing list for other than official university business without his or her consent. Mailing lists may be used only for their intended purposes.
- 2.04 All materials sent by campus email must be attributed to the individual, office, or organization sending the material. It is a violation of this policy to originate email in such a manner as to create the impression to the recipient that the mail was originated from another source or individual.

OSU INSTITUTE OF TECHNOLOGY
POLICY & PROCEDURES

- 2.05 Any OSUIT employee may send email, relating to university business, to individual employees from their individually assigned university email account. Director level or above authorization is required to send emails to all students or all employees.
- 2.06 A limited number of offices will have access to send emails to students through departmental service accounts.
- 2.07 The OSUIT Communications service account and the use of the name “OSUIT Communications” is restricted to the Office of Marketing & Communications for the purpose of institutional communications both internally and externally. Its use is solely at the discretion of the Director of Marketing & Communications.

Issues Related to Privacy

3.01 General Policy Statements

- A. It is the intent of the university to preserve the privacy of email communications and maintain access to communications intended for an individual. Given that universities place high value on open communication of ideas, including those new and controversial, the intention of the university is to maximize freedom of communication for purposes that further the goals of the university.
- B. All email communications, unless subject to a specific privilege, are subject to production under the Oklahoma Open Records Act and, when relevant, to discovery in civil litigation.

3.02 Individual Expectations

- A. Email messages shall be delivered to the addresses and not censored or interfered with in any way by the university.
- B. Individually addressed email communications may not be read by any third party except as noted below. Any access of individual email communications other than that noted below is in violation of university policy and action will be taken accordingly.

3.03 University Requirements

- A. University officers and supervisors shall have the right to read any email when written permission for such access has been given by the individual.
- B. Under certain circumstances a system administrator may, in the course of his or her professional duties, access an individual's email for legitimate management or maintenance purposes.

OSU INSTITUTE OF TECHNOLOGY
POLICY & PROCEDURES

- C. If an occasion arises when a university officer or supervisor believes that access to an individual's email account is required for the conduct of university business, the university individual is not available, and a system administrator is required to access the individual's email account, the following procedure shall be followed:
1. The university official or supervisor shall secure permission to access the email account from the Associate Vice President of Technology Services.
 2. An appropriate form with the signature of the Associate Vice President of Technology Services shall be presented to the system administrator allowing the system administrator to proceed to access the email account.
 3. The individual whose email account has been accessed will be notified as soon as possible by copy of the above referenced form.
- D. Keeping in mind the university's intent to preserve the privacy of email, if an occasion arises when a university officer or supervisor believes that access to an individual's email account is required because there is reason to believe the individual is engaged in wrongdoing, and a system administrator is required to access the individual's email account, steps 3.03A and 3.03B above shall be followed. The individual whose email account has been accessed will be notified upon conclusion of the monitoring process. Such notification shall be made in a timely manner.
- E. Prior to separation, resignation, or transfer, faculty and staff members are expected to make all email files related to university business available to their supervisor.
- F. Upon separation or resignation, the individual's email account will be deactivated and all information not retained by the supervisor will be deleted according to the retention policy at the time. Employees who are separated or resign, who go on to employment at another OSU System school, or who have a student role also, will continue to have access to their university email.
- G. Because emails sent and received in the course of an employee's university employment belong to the university, and are subject to the Open Records Act and other discovery requests, employees must use the university provided email account for university business. Automatic mass redirecting or forwarding of email to a non-university account is not allowed.
- H. University-owned employee email accounts should use the standardized template with logo and formatting so that university emails have a consistent look and feel. Custom words of wisdom and special backgrounds should not be used.

OSU INSTITUTE OF TECHNOLOGY
POLICY & PROCEDURES

Access to University Electronic Mail Accounts

- 4.01 When a member of the university community activates their O-Key account, an email account will be created and made available for their use. This does not guarantee unlimited or unrestricted opportunities to use the email account. By using university email services, one agrees to comply with all university policies, procedures, and local, state, and federal laws, including but not limited to trademark, patent, copyright, and trade secret laws.
- 4.02 While account holders may expect reasonable access to email, this cannot be guaranteed to be at all times and in all circumstances.
- 4.03 Violation of this policy may result in the loss of email privileges at this university.

Objectionable Material, Violations and Sanctions

- 5.01 The university cannot protect individuals against the existence or receipt of material that may offend them. Those who make use of email are warned that they may willingly or unwillingly come across, or be recipients of, material that they may find offensive. Members of the university community are expected to demonstrate good taste and sensitivity to others in their communications. While every effort is made to filter spam, objectionable material, and fraudulent emails, the individual must make an effort to avoid opening or responding to emails that seem strange, come from unknown persons or organizations, or ask for information of a confidential nature. Periodically, alerts will be sent out to the university community warning of dangerous or fraudulent email.
- 5.02 It is a violation of this policy to use email to libel, harass, or threaten other individuals.

Approved: October 2004
Revised: July 2009
Revised: August 2013
Revised: July 2016
Revised: December 2019